Avid MediaCentral Platform Services

Upgrade Guide

Version 2.10

Legal Notices

Product specifications are subject to change without notice and do not represent a commitment on the part of Avid Technology, Inc.

This product is subject to the terms and conditions of a software license agreement provided with the software. The product may only be used in accordance with the license agreement.

This product may be protected by one or more U.S. and non-U.S patents. Details are available at www.avid.com/patents.

This guide is protected by copyright. This guide is for your personal use and may not be reproduced or distributed, in whole or in part, without permission of Avid. Reasonable care has been taken in preparing this guide; however, it may contain omissions, technical inaccuracies, or typographical errors. Avid Technology, Inc. disclaims liability for all losses incurred through the use of this document. Product specifications are subject to change without notice.

Copyright © 2017 Avid Technology, Inc. and its licensors. All rights reserved.

The following disclaimer is required by Apple Computer, Inc.:

APPLE COMPUTER, INC. MAKES NO WARRANTIES WHATSOEVER, EITHER EXPRESS OR IMPLIED, REGARDING THIS PRODUCT, INCLUDING WARRANTIES WITH RESPECT TO ITS MERCHANTABILITY OR ITS FITNESS FOR ANY PARTICULAR PURPOSE. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME STATES. THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY PROVIDES YOU WITH SPECIFIC LEGAL RIGHTS. THERE MAY BE OTHER RIGHTS THAT YOU MAY HAVE WHICH VARY FROM STATE TO STATE.

The following disclaimer is required by Sam Leffler and Silicon Graphics, Inc. for the use of their TIFF library:

Copyright © 1988–1997 Sam Leffler
Copyright © 1991–1997 Silicon Graphics, Inc.

Permission to use, copy, modify, distribute, and sell this software [i.e., the TIFF library] and its documentation for any purpose is hereby granted without fee, provided that (i) the above copyright notices and this permission notice appear in all copies of the software and related documentation, and (ii) the names of Sam Leffler and Silicon Graphics may not be used in any advertising or publicity relating to the software without the specific, prior written permission of Sam Leffler and Silicon Graphics.

THE SOFTWARE IS PROVIDED “AS-IS” AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IN NO EVENT SHALL SAM LEFFLER OR SILICON GRAPHICS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The following disclaimer is required by the Independent JPEG Group:

This software is based in part on the work of the Independent JPEG Group.

This Software may contain components licensed under the following conditions:

Copyright (c) 1989 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright (C) 1989, 1991 by Jef Poskanzer.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. This software is provided "as is" without express or implied warranty.

Copyright 1995, Trinity College Computing Center. Written by David Chappell.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. This software is provided "as is" without express or implied warranty.

Copyright 1996 Daniel Dardailler.

Permission to use, copy, modify, distribute, and sell this software for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Daniel Dardailler not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Daniel Dardailler makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Modifications Copyright 1999 Matt Koss, under the same license as above.

Copyright (c) 1991 by AT&T.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHOR NOR AT&T MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

This product includes software developed by the University of California, Berkeley and its contributors.

The following disclaimer is required by Paradigm Matrix:

Portions of this software licensed from Paradigm Matrix.

The following disclaimer is required by Ray Sauers Associates, Inc.:

“Install-It” is licensed from Ray Sauers Associates, Inc. End-User is prohibited from taking any action to derive a source code equivalent of “Install-It,” including by reverse assembly or reverse compilation, Ray Sauers Associates, Inc. shall in no event be liable for any damages resulting from reseller’s failure to perform reseller’s obligation; or any damages arising from use or operation of reseller’s products or the software; or any other damages, including but not limited to, incidental, direct, indirect, special or consequential Damages including lost profits, or damages resulting from loss of use or inability to use reseller’s products or the software for any reason including copyright or patent infringement, or lost data, even if Ray Sauers Associates has been advised, knew or should have known of the possibility of such damages.

The following disclaimer is required by Videomedia, Inc.:

“Videomedia, Inc. makes no warranties whatsoever, either express or implied, regarding this product, including warranties with respect to its merchantability or its fitness for any particular purpose.”

“This software contains V-LAN ver. 3.0 Command Protocols which communicate with V-LAN ver. 3.0 products developed by Videomedia, Inc. and V-LAN ver. 3.0 compatible products developed by third parties under license from Videomedia, Inc. Use of this software will allow “frame accurate” editing control of applicable videotape recorder decks, videodisc recorders/players and the like.”

The following disclaimer is required by Altura Software, Inc. for the use of its Mac2Win software and Sample Source Code:

©1993–1998 Altura Software, Inc.

The following disclaimer is required by 3Prong.com Inc.:

Certain waveform and vector monitoring capabilities are provided under a license from 3Prong.com Inc.

The following disclaimer is required by Interplay Entertainment Corp.:

The “Interplay” name is used with the permission of Interplay Entertainment Corp., which bears no responsibility for Avid products.

This product includes portions of the Alloy Look & Feel software from Incors GmbH.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

© DevelopMentor

This product may include the JCifs library, for which the following notice applies:

JCifs © Copyright 2004, The JCIFS Project, is licensed under LGPL (http://jcifs.samba.org/). See the LGPL.txt file in the Third Party Software directory on the installation CD.

Avid Interplay contains components licensed from LavanTech. These components may only be used as part of and in connection with Avid Interplay.

Portions © Copyright 2003-2007 of MOG Solutions.

Attn. Government User(s). Restricted Rights Legend

U.S. GOVERNMENT RESTRICTED RIGHTS. This Software and its documentation are “commercial computer software” or “commercial computer software documentation.” In the event that such Software or documentation is acquired by or on behalf of a unit or agency of the U.S. Government, all rights with respect to this Software and documentation are subject to the terms of the License Agreement, pursuant to FAR §12.212(a) and/or DFARS §227.7202-1(a), as applicable.

Trademarks

Avid, the Avid Logo, Avid Everywhere, Avid DNXHD, Avid DNXHR, Avid Nexis, AirSpeed, Eleven, EUCON, Interplay, iNEWS, ISIS, Mbox, MediaCentral, Media Composer, NewsCutter, Pro Tools, ProSet and RealSet, Maestro, PlayMaker, Sibelius, Symphony, and all related product names and logos, are registered or unregistered trademarks of Avid Technology, Inc. in the United States and/or other countries. The Interplay name is used with the permission of the Interplay Entertainment Corp. which bears no responsibility for Avid products. All other trademarks are the property of their respective owners. For a full list of Avid trademarks, see: http://www.avid.com/US/about-avid/legal-notices/trademarks.

Footage

WCAU Fire Story — Courtesy of NBC-10, Philadelphia, PA.

News material provided by WFTV Television Inc.

Avid MediaCentral Platform Services Upgrade Guide • Created July 27, 2017 • This document is distributed by Avid in online (electronic) form only, and is not available for purchase in printed form.

Contents

Using This Guide 7
Symbols and Conventions 7
If You Need Help. 8
Avid Training Services 8
Chapter 1 **Overview and Prerequisites** 9
Overview 10
How to Use this Guide 10
Obtaining the Software Packages. 10
Mounting the Operating System 11
Upgrading Multi-Zone Deployments 12
Upgrading Media | Index Deployments. 13
Upgrading the Avid Shared Storage Client 14
Upgrading the MediaCentral Distribution Service 15
Upgrading the iNEWS Client Version 15
An Important Note on SSL Certificates 16
Backing Up and Restoring SSL Private Keys 16
Migrating User Settings from UMS to USS During an Upgrade 17
Upgrade Prerequisites 17
Upgrade Paths 18
Chapter 2 **Upgrades for RHEL v6.5 Systems** 19
Upgrading a RHEL 6.5 Single Server to MCS v2.10 19
Upgrading to MCS v2.10 19
Continuing the Upgrade 21
Upgrading a RHEL 6.5 Cluster System to MCS v2.10 24
Identifying the Master, Slave and Load-Balancing Nodes 24
Backing-up the User Database and System Settings 25
Additional Steps for Systems with Media Index 25
Taking the Cluster Offline. 26
Updating the Cluster 26
Stopping the RabbitMQ Service and Rebooting the Cluster 28
Verifying the RabbitMQ Cluster 29
Bringing the Corosync Cluster Online 29
Continuing the Upgrade 31
(if applicable) Verifying Gluster Volume Permissions 33

(if applicable) Removing the Gluster Metadata Cache Replication Volume. 34
Chapter 3 Upgrades for RHEL v6.3 Systems 35
Upgrading a RHEL 6.3 Single Server to MCS v2.10 35
Backing-up System Settings 35
Installing RHEL 6.5 and MCS 2.10 36
Restoring System Settings and Migrating the User Database 37
Additional Upgrade Procedures 38
Upgrading a RHEL 6.3 Cluster System to MCS v2.10 40
Identifying the Master, Slave and Load-Balancing Nodes 40
Backing Up the System Settings. 40
Taking the Cluster Offline 41
Upgrading the Software 42
Restoring System Settings and Migrating the User Database 43
Additional Upgrade Procedures 44
Chapter A Post Upgrade Notes 47
Configuring MCS System Settings 47
Verifying the ACS Gateway Port for Interplay | MAM 47
Reconfiguring MCS for Upgrades from ICS v1.7 or Earlier 47
Resetting Layouts After Upgrading from v2.0 to v2.10 49
Resetting Layouts After Upgrading from ICS v1.6 or Earlier 49
Clearing the Browser Cache 50
Clearing the Cache in Chrome. 50
Clearing the Cache in Safari 50
Chapter B Mounting and Unmounting a USB Drive 51
Chapter C Copying Software to the MCS Server 53
Copying Software Using WinSCP. 53
Copying Software Using a USB Drive. 54
Chapter D Deleting the RAID 5 Array 55
Deleting the RAID 5 on an HP Gen9 55
Deleting the RAID 5 on an HP Gen8 56
Deleting the RAID 5 on a Dell Server 59
Chapter E Working with Media Index 63
Verifying the Media Index Status 63
Stopping and Starting the PEBCo Agent 64
Stopping the PEBCo Agent 64
Starting the PEBCo Agent 64
Chapter F Verifying System Configuration Files 65
Chapter G Backing Up and Restoring System Settings and the ICS/MCS Database 67
Completing a Backup 68

Completing a Restore 69

Using This Guide

This document provides instructions for upgrading to MediaCentral Platform Services (MCS) v2.10 from a previous version of MCS or Interplay Central Services (ICS).

To complete a new installation of MediaCentral Platform Services, see the *MediaCentral Platform Services Installation and Configuration Guide*. For administrative information for MediaCentral | UX, see the *Avid MediaCentral | UX Administration Guide*.

Symbols and Conventions

Avid documentation uses the following symbols and conventions:

Symbol or Convention	Meaning or Action
	A note provides important related information, reminders, recommendations, and strong suggestions.
	A caution means that a specific action you take could cause harm to your computer or cause you to lose data.
	A warning describes an action that could cause you physical harm. Follow the guidelines in this document or on the unit itself when handling electrical equipment.
>	This symbol indicates menu commands (and subcommands) in the order you select them. For example, File > Import means to open the File menu and then select the Import command.
‣	This symbol indicates a single-step procedure. Multiple arrows in a list indicate that you perform one of the actions listed.
(Windows), (Windows only), (Macintosh), or (Macintosh only)	This text indicates that the information applies only to the specified operating system, either Windows or Macintosh OS X.
Bold font	Bold font is primarily used in task instructions to identify user interface items and keyboard sequences.
Italic font	Italic font is used to emphasize certain words and to indicate variables.
`Courier Bold font`	Courier Bold font identifies text that you type.
Ctrl+key or mouse action	Press and hold the first key while you press the last key or perform the mouse action. For example, Command+Option+C or Ctrl+drag.

If You Need Help

If you are having trouble using your Avid product:

1. Retry the action, carefully following the instructions given for that task in this guide. It is especially important to check each step of your workflow.
2. Check the latest information that might have become available after the documentation was published. You should always check online for the most up-to-date release notes or ReadMe because the online version is updated whenever new information becomes available. To view these online versions, select ReadMe from the Help menu, or visit the Knowledge Base at www.avid.com/support.
3. Check the documentation that came with your Avid application or your hardware for maintenance or hardware-related issues.
4. Visit the online Knowledge Base at www.avid.com/support. Online services are available 24 hours per day, 7 days per week. Search this online Knowledge Base to find answers, to view error messages, to access troubleshooting tips, to download updates, and to read or join online message-board discussions.

Avid Training Services

Avid makes lifelong learning, career advancement, and personal development easy and convenient. Avid understands that the knowledge you need to differentiate yourself is always changing, and Avid continually updates course content and offers new training delivery methods that accommodate your pressured and competitive work environment.

For information on courses/schedules, training centers, certifications, courseware, and books, please visit www.avid.com/support and follow the Training links, or call Avid Sales at 800-949-AVID (800-949-2843).

1 Overview and Prerequisites

Avid recommends that you read all the information in the *Avid MediaCentral Platform Services ReadMe* and the *Avid MediaCentral Platform Services Upgrade Guide* thoroughly before installing or using the corresponding software release.

Important: Check the v2.10 documentation landing page for the latest updates to this guide and all related documentation for Avid MediaCentral Platform Services:

http://avid.force.com/pkb/articles/en_US/readme/Avid-MediaCentral-Version-2-10-x-Documentation

For a list products qualified for use with MCS v2.10, and the supported RHEL operating system, see the Software Compatibility Matrix on the Avid Knowledge Base.

Revision History

Date Revised	Changes Made
July 28, 2017	The process for Upgrading a RHEL 6.5 Cluster System to MCS v2.10 has been clarified to list the Media Distribute and Assignments Pane upgrades as steps that must occur after the cluster is back online.
April 27, 2017	Two new health check steps have been added to the list of "Upgrade Prerequisites" on page 17.
March 30, 2017	Initial release. • Some steps related to the avid-acs-gateway service added to the MCS v2.9.0 Upgrade Guide have been removed as the steps are no longer required.

Overview

The MediaCentral Platform Services (MCS) upgrade process includes a migration of custom settings, databases and system files. Depending on your upgrade path, the migration of settings and data is either manual or automated.

There are two main upgrade paths to MCS v2.10, depending on the currently installed version of the Red Hat Enterprise Linux (RHEL) operating system:

- RHEL v6.5 – If this is the currently installed operating system, the upgrade is non-destructive and the process is largely automated. Creating a manual back-up of the MCS database and system settings is recommended, but not required.
- RHEL v6.3 and earlier – If this is the currently installed operating system, the process is closer to a new installation than it is to an upgrade. Users must use the MCS Installation USB Drive to re-image the server and complete a fresh installation of RHEL and MCS. Because of this, extra care must be taken to ensure the MCS system settings and user database are preserved.

  Creating a manual back up of the MCS database and system settings is mandatory. This backup process must be completed before the upgrade and a manual restoration of the data is required once the upgrade is complete. You must also manually back up any private keys associated with SSL certificates received from a Certificate Authority, if CA-signed certificates are in use. In the case of a cluster, you must manually re-create the Corosync cluster and reconfigure Gluster cache replication (if applicable).

How to Use this Guide

This guide documents the overall upgrade process for the supported upgrade scenarios. It must be used in conjunction with the *MediaCentral Platform Services Installation and Configuration Guide*.

For each step in the overall upgrade process, this document offers the following guidance:

- Includes step-by-step instructions for a procedure.

  - or -

- Cross-references a section in an separate document such as the *MediaCentral Platform Services Installation and Configuration Guide*.

In the second case, the heading of the relevant section of the document is provided. Since direct page references are unreliable, you must scan the table of contents in that guide to find the heading and page.

If copying / pasting commands from this document into a command line interface such as Putty, be sure to verify the command after pasting. It is possible that some characters might be replaced during the paste process which can lead to a failed or problematic installation.

Obtaining the Software Packages

Multiple software packages are required to properly install and configure MediaCentral Platform Services. For more information on downloading these packages, see “Obtaining the Software” in the *MediaCentral Platform Services Installation and Configuration Guide*.

Mounting the Operating System

Whether performing an upgrade or a full installation, the MCS installer requires the RHEL ISO to be mounted to the `/sysinstall` directory on the MCS server. This is true, even when performing an upgrade where the operating system does not change. The body of this guide assumes that you are completing the upgrade using the MCS Installation USB Drive. In this case the RHEL ISO is automatically mounted during the upgrade procedure.

MCS systems in a virtual environment often do not use USB drives. In these cases, the RHEL.ISO must be mounted as either a file or as a disk in a virtual optical drive. This section details three different methods for mounting the RHEL.ISO.

To mount the RHEL.ISO from the MCS Installation USB Drive:

1. Refer to the process in Appendix B: Mounting and Unmounting a USB Drive.

   This process is generally used in hardware-based environments, but it could also be used with virtual machines equipped with a virtual USB port.

To mount the RHEL.ISO as a file:

1. Copy the RHEL.ISO to a directory on the MCS server such as `/tmp` or `/media`.
2. Use the following command to mount the ISO to the `/sysinstall` directory:

   `mount -o loop /<path>/<filename> /sysinstall`

   For example:

   `mount -o loop /media/rhel-server-6.5-x86_64-dvd.iso /sysinstall`

Once you have completed the upgrade, be sure to unmount the ISO from the `/sysinstall` directory using the Linux umount command. For example: `umount /sysinstall`

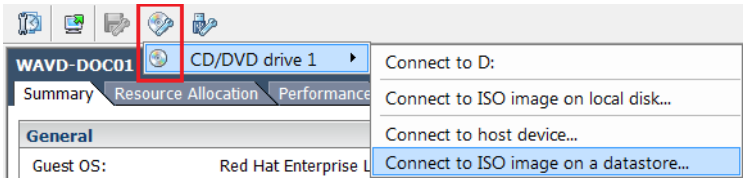
To mount the RHEL.ISO as a virtual optical drive:

1. Copy the RHEL.ISO to a directory on your virtual environment's datastore.

   For instructions, see the documentation for your virtual environment.

2. Mount the ISO as a virtual optical drive.

   For example, in the v6.0 vSphere VMware thick client, you would select the button to "Connect/disconnect the CD/DVD devices of the virtual machine" and chose to "Connect to ISO image on a datastore..." from the menu as indicated below:



3. Once the ISO is mounted to the virtual optical drive, you must mount the image to the `/sysinstall` directory:

   `mount /dev/cdrom /sysinstall`

Once you have completed the upgrade, be sure to unmount the ISO from the `/sysinstall` directory using the Linux umount command. For example: `umount /sysinstall`

Upgrading Multi-Zone Deployments

If your system is configured for a multi-zone environment, note the following:

- As multi-zone configurations often span WAN (wide area network) environments, special attention should be paid to ensure that the correct network ports are open between the zones. Review the Avid Networking Port Usage Guide on the Avid Knowledge Base for more information on the ports required for multi-zone.
- If you are upgrading from MCS v2.3.x or earlier, after the master zone has been updated, the `/opt/avid/cluster/bin/pgpool_remote_start` script needs to be run to enable the proper syncing of the user databases between all zones again. Be aware that the script will restart some services on the systems in the remote zones. After the services are restarted, users must sign back into MediaCentral UX.
- If you are upgrading from MCS v2.3.x or earlier, upgrade slave zones first. If you cannot bring all zones offline at the same time, upgrade the slave zone(s) before the master zone.

  An upgraded MCS v2.3 slave zone no longer has access to the centralized user management service (UMS), which is owned by the master zone. Users in the upgraded slave zone can continue to sign in using the local, read-only copy of the UMS database. However, new users cannot be added through the slave zone.
- If you are upgrading from MCS v2.4.x or later, upgrade the master zone first. Once the master zone has been upgraded, you can upgrade the slave zones in any order. Slave zones running MCS v2.4.x will continue to be able to access the master zone's user database and will not be limited to read-only mode as in previous releases.

Although slave zones running v2.4 - v2.6.x can read the user database in a master zone running v2.10, these versions are not supported in a mixed multi-zone configuration. Zones running MCS v2.6.x and earlier must be upgraded to a compatible software release.

- Master and slave zones running MCS v2.8.x, and v2.9.x are supported operating in a mixed environment with zones running MCS v2.10.
- If you are upgrading a zone that was running MCS v2.5.x or earlier and your multi-zone configuration contains zones that are running v2.6 or later and have already been configured for sharded Mongo, make sure to add the new zone to the sharded Mongo configuration.

  For details, see "Adding a Zone to a Sharded Mongo Multi-Zone Environment" in the *MediaCentral Platform Services Installation and Configuration Guide*.

Upgrading Media | Index Deployments

If your deployment is configured for Media Index, note the following:

- If your upgrade includes an index schema migration, note that the process can take multiple hours to complete on large systems. During this time, indexed searching (with the exception of marker searches) is functional, but slow. Additionally, systems cannot add data to the index through the indexing agents while the migration occurs. Administrators might consider stopping the indexing agents during this period.
- If you are upgrading from MediaCentral v2.1.x or earlier, the indexes are incompatible with MediaCentral v2.10. Before upgrading to MCS v2.10, you must reset the Media Index configuration and delete the indexes in all zones. Deleting the indexes reverts the index table to a clean (empty) state.

  For instructions, see "Upgrading Media Index from v2.0.x or v2.1.x" the *Avid Media | Index Configuration Guide*.
- If you are upgrading from MediaCentral v2.2.x or v2.3.x, the indexes are compatible with MediaCentral v2.10 and do not need to be deleted. However, a migration script (`media-index-upgrade.sh`) must be run before upgrading to v2.10 to update the schema to include new features associated with MCS v2.10. Once the system is upgraded to v2.10, a second script (`avid-acs-mediaindex-indices-migration`) must be run to complete the process.

  Details for running the migration scripts are contained in the body of this document.
- If you are upgrading from MediaCentral v2.4.0 or later, the indexes are compatible with MediaCentral v2.10 and do not need to be deleted. However, a migration script must be run after upgrading to v2.10. The script updates the schema to include new features associated with MCS v2.10.

  Details for running the migration script is contained in the body of this document.
- If you are upgrading from a version of MCS prior to v2.3.2.5, v2.4.2.4, v2.5.4, v2.6.2.3, or v2.7.1.3, you must first stop the PEBCo agent in the Interplay Administrator to pause the indexing of the Interplay Production or Interplay Archive database. Once the upgrade is complete, the PEBCo agent must be manually restarted.

  The body of this guide instructs you to complete this process at the appropriate time during the upgrade. For full details, see "Stopping and Starting the PEBCo Agent" on page 64.
- To configure the Production Engine Bus Connector (PEBCo) for Media Index with MCS v2.10, you must use the Interplay Administrator tool v3.5 or later. If you are indexing an Interplay Archive database, Interplay Administrator v3.6 or later is required.

The Interplay Administrator is co-installed with Interplay Access. The required version of Access must be installed somewhere in your network; it does not necessarily have to be the instance of Access on the Interplay Engine. If installing an alternate version of Access, it is this instance of the software that must be used to configure PEBCo.

Upgrading the Avid Shared Storage Client

During the MediaCentral Platform Services installation process, a version of the Avid shared storage client software is automatically installed. When upgrading to MCS v2.10, the following upgrade scenarios apply:

- If your system is already running the Avid NEXIS client, the latest version of the Avid NEXIS client is automatically installed if necessary. No additional steps are required.
- If your system is already running the Avid ISIS client, the latest version of the Avid ISIS client is automatically installed if necessary. No additional steps are required.
- If you are upgrading a system running the Avid ISIS client and you plan to either add Avid NEXIS shared storage to the configuration or transition from Avid ISIS to Avid NEXIS, you must manually upgrade the Avid shared storage client.

Once the MediaCentral Platform Services upgrade is complete, verify the version of the shared storage client required for your configuration and upgrade the client if necessary. For more information on client version compatibility, see the Compatibility Matrix: Interplay Production and MediaCentral on the Avid Knowledge Base.

To upgrade the shared storage client:

1. Prior to upgrading the shared storage client, you must first stop the ICPS back-end services that use the storage client:
   - For a single server, use the following command:

     `service avid-all stop`
   - For clustered configurations, issue the following command from any node to stop the cluster resource that manages the service:

     `crm resource stop AvidAllEverywhere`
2. Navigate to the location of the bundled shared storage client software:

   `cd /opt/avid/Packages`
3. Use the following command to upgrade the shared storage client:

   `rpm -Uvh AvidNEXISClient-<version>.el6.x86_64.rpm`

   You do not need to uninstall any previous version of the client software. The installer automatically replaces the version of the client already installed on the system.

   If you are running a cluster configuration, repeat this command on each cluster node.
4. Once the client is installed, restart the avid-all service:
   - For a single server, use the following command:

     `service avid-all start`
   - For clustered configurations, issue the following command from any cluster node:

     `crm resource start AvidAllEverywhere`

Upgrading the client on a cluster might introduce resource fail-counts. Use the Cluster Resource Monitor, `crm_mon`*, to verify the status of the cluster and if necessary, clear the fail-counts with the* `crm resource cleanup <rsc> [<node>]` *command.*

5. Verify the version number of the updated client software:

   ```
   rpm -qa | egrep -i 'isis|nexis'
   ```

   This command returns all installed packages with either ISIS or NEXIS in the name.

Upgrading the MediaCentral Distribution Service

The MediaCentral Distribution Service (MCDS) is used in MediaCentral UX configurations which employ a Send To Playback (STP) workflow. Consult the version compatibility chart on the Avid Knowledge Base for the correct version of MCDS for your installation and upgrade the software if necessary.

http://avid.force.com/pkb/articles/en_US/compatibility/Avid-Video-Compatibility-Charts

To upgrade the MediaCentral Distribution Service:

1. The MediaCentral Distribution Service could be in one or more locations within your environment. Use the following process to verify where MCDS is installed:
   a. Sign in to MediaCentral UX as a user with administrator-level access.

      See “Signing into MediaCentral” in the *MediaCentral Platform Services Installation and Configuration Guide* for additional information.

   b. Select System Settings from the Layout selector.
   c. In the Settings pane, select Interplay | Production.
   d. Make note of the MCDS Service URL. This field lists the location or locations where MCDS has been installed.
   e. Log out of MediaCentral UX and close the browser.
2. On the system or systems where MCDS has been installed, use the Windows Control Panel to uninstall the MCDS software.

MCDS v3.3 and later are 64 bit applications. Prior 32 bit versions of MCDS must be manually removed to avoid the installation of multiple versions on the same system.

3. If you are upgrading from a 32 bit version of MCDS, navigate to C:\Program Files (x86)\Avid\ and delete the residual “MediaCentral Distribution Service” folder.
4. Install the updated version of MCDS.
5. Repeat this process if you need to upgrade MCDS on a second host system.

Upgrading the iNEWS Client Version

If your workflow includes integration with Avid iNEWS, ensure that your iNEWS system is updated with the iNEWS client version for this release of MCS. See “iNEWS Client Version” in the *Avid MediaCentral Platform Services ReadMe* for iNEWS client version information. See “Editing SYSTEM.CLIENT.VERSIONS” in the *MediaCentral Platform Services Installation and Configuration Guide* for instructions on adding the client version to the iNEWS server.

An Important Note on SSL Certificates

MediaCentral Platform Services uses the Secure Sockets Layer (SSL) for its server to browser connections.

MCS v2.5 uses a different SSL certificate format than found in previous releases. If you are upgrading to MCS v2.5 or later and using a Self-Signed or Trusted-CA certificate, refer to the following article on the Avid Knowledge Base to create or in some cases upgrade your SSL certificate:

http://avid.force.com/pkb/articles/en_US/how_to/SSL-Certificates-for-server-to-browser-connections

Changes to the application.properties file (/opt/avid/etc/avid/avid-interplay-central/config/application.properties) required for Jetty certificates in MCS v2.4 and earlier are no longer required. If desired, the changes can be reverted after the upgrade to MCS v2.5 or later. Alternatively, the application.properties file can remain unaltered and the Jetty certificate information will be ignored.

Backing Up and Restoring SSL Private Keys

Upgrading can be a “true” (non-destructive) upgrade, or can involve a fresh install of RHEL. For fresh installations, a script has been provided to back up and restore system settings related to MCS, including SSL data (the certificate and associated private key).

However, if you are using a Trusted CA-signed Certificate, a private key (site.key or jettyPrivateKey.key) file was created during the certificate creation process. The creation procedure suggests that you back up this file in a safe place, such as the root user home directory (`/root`) directory. If you are performing a fresh install of RHEL, be sure to backup this private key to an external location before performing the upgrade. Backing up private key files is good practice, whatever the type of upgrade being performed.

If the private key was not backed up elsewhere, it is doubly important to back up the file before performing the upgrade. The private key is used to generate Certificate Signing Requests (CSRs).

For instructions on creating and installing SSL certificates see the following article:

http://avid.force.com/pkb/articles/en_US/how_to/SSL-Certificates-for-server-to-browser-connections

To back up and restore the private key file:

1. Locate the private key file used to generate the Certificate Signing Request (if any). The Avid provided SSL creation process suggests that you store the key in the following directory:

   `/root`

   The default file name for MCS v2.5 and later is `site.key`. The default file name for MCS v2.4 and earlier is `jettyPrivateKey.key`.
2. Copy the private key to an external location such as a network share or a USB drive.
3. If applicable, restore the key at the appropriate step in the upgrade.

Migrating User Settings from UMS to USS During an Upgrade

MediaCentral Platform Services v2.0 introduced a new user database scheme. Upgrades of systems running MCS v2.0 or earlier must complete a user database migration using the supplied avid-uss-import script.

- For upgrades from v1.8.0 (RedHat v6.3) or earlier, a backup and restore of the MCS database is required. The user database migration must be completed after restoring the MCS database, but before logging in via the MediaCentral UX user interface.
- For upgrades from v1.8.1 (RedHat v6.5), a backup and restore of the MCS database is not required. However, the avid-uss-import script must still be run before logging in via the MediaCentral UX user interface.

In a cluster, the user database migration script must be run once on the master node only.

For more information on backup and restore procedures, see "Backing Up and Restoring System Settings and the ICS/MCS Database" on page 67. Procedures for using the avid-uss-import script are covered in "Upgrades for RHEL v6.3 Systems" on page 35.

Upgrade Prerequisites

Before starting any MCS upgrade, it is important to ensure you have a healthy environment. Verify the following as appropriate:

- (All configurations) Ensure you can sign in to MediaCentral UX through a supported web browser and verify basic functionality.
- (Cluster configurations) Verify the status of RabbitMQ and the ACS Bus.

  For details, see "Verifying the Status of RabbitMQ" in the *MediaCentral Platform Services Installation and Configuration Guide*.
- (Cluster configurations) Verify the status of the Corosync cluster. Ensure there are no errors.

  For details, see "Cluster Resource Monitor" in the *MediaCentral Platform Services Concepts and Clustering Guide*.
- (Multi-zone configurations) Verify that the "Zones" section of the MediaCentral UX System Settings layout displays all expected zones with no errors.

  For details, see "Troubleshooting the Multi-Zone Setup" in the *MediaCentral Platform Services Installation and Configuration Guide*.
- If you are upgrading from MediaCentral Platform Services v2.6 or later, verify that your sharded MongoDB configuration is operating normally.

  For details, see "Obtaining the Status of Sharded Mongo" in the *MediaCentral Platform Services Installation and Configuration Guide*.
- If you are upgrading from MediaCentral Platform Services v2.7 or later, use the avid-system-check script to verify the overall heath of the system.

  For details, see "Using the MediaCentral Health Check Script" in the *MediaCentral Platform Services Installation and Configuration Guide*.

- Specific security updates have been approved by Avid for use with MediaCentral Platform Services running on Red Hat Enterprise Linux. Avid recommends installing these updates on all MCS servers.

  At minimum, sites upgrading to MCS v2.9 and later are **required** to install the Open SSL "Heartbleed" security update v1.0.1e-30.el6_6.5 or later prior to upgrading the MediaCentral software.

  For more information about approved security updates, see the "Security Updates" section of the *Avid MediaCentral Platform Services ReadMe*.

Upgrade Paths

Refer to one of the following sections to upgrade MediaCentral Platform Services:

Upgrades for systems already running Red Hat Enterprise Linux (RHEL) v6.5

For upgrading instructions:

- "Upgrading to MCS v2.10" on page 19
- "Upgrading a RHEL 6.5 Cluster System to MCS v2.10" on page 24

Upgrades for systems running Red Hat Enterprise Linux (RHEL) v6.3

For upgrading instructions:

- "Upgrading a RHEL 6.3 Single Server to MCS v2.10" on page 35
- "Upgrading a RHEL 6.3 Cluster System to MCS v2.10" on page 40

2 Upgrades for RHEL v6.5 Systems

If upgrading a MediaCentral Platform Services system already running RHEL v6.5, refer to one of the following two processes:

- Upgrading a RHEL 6.5 Single Server to MCS v2.10
- Upgrading a RHEL 6.5 Cluster System to MCS v2.10

Prior to upgrading, ensure you have verified the "Upgrade Prerequisites" on page 17.

MCS v2.6.0 and later requires sharded MongoDB to be configured on MediaCentral systems in clustered or multi-zone environments. If your system has already been configured with sharded MongoDB, a reconfiguration might be required for certain upgrade paths. The process for configuring sharded Mongo is referenced in the upgrade process below.

Upgrading a RHEL 6.5 Single Server to MCS v2.10

Installing MCS v2.10 on a single server already operating under RHEL v6.5 involves an automated update of the affected packages. All MCS system settings are preserved.

Estimated downtime: 1 hour

The single-server upgrade involves the following steps:

- Upgrading to MCS v2.10
- Continuing the Upgrade

Upgrading to MCS v2.10

Installing MCS v2.10 on a single server already operating under RHEL v6.5 involves an automated update of the affected packages. All MCS system settings are preserved.

To install MediaCentral Platform Services v2.10:

1. Prepare the v2.10 MCS Installation USB Drive and connect it to your MCS server.

   It is necessary to upgrade the system using the MCS Installation USB Drive as it contains the RHEL v6.5 ISO required for the upgrade process.

   For details on preparing the USB drive, see "Creating the MCS Installation USB Drive" in the *MediaCentral Platform Services Installation and Configuration Guide*.

2. Mount the USB drive and change to the USB mount point.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

The MCS Installation USB Drive contains all software used to image a new MediaCentral server. Do not reboot the server with this USB drive attached!

3. Although the upgrade is non-destructive, it is a good idea to back-up the MCS database. This is an optional, but recommended step.

   Create a back-up of the MCS settings and database using the script located on the USB drive:

   `./system-backup.sh -b`

   For additional detail on using this script, see "Backing Up and Restoring System Settings and the ICS/MCS Database" on page 67.

4. (Media Index configurations only) If you are upgrading from MCS v2.2.x or v2.3.x, you need to run a schema migration script before upgrading the MCS software.

   a. Prior to running the migration script, review "Verifying the Media Index Status" on page 63 to ensure that no active schema migration is currently affecting Media Index.

   b. Once you have verified the status, run the migration script from the root of the MCS Installation USB Drive:

      `./media-index-upgrade.sh`

   This script will update the indexes to be compatible with the MCS v2.10 index structure.

The elasticsearch service must be running for this script to complete the migration tasks.

5. (Media Index configurations only) If you are upgrading from a version of MCS prior to v2.3.2.5, v2.4.2.4, v2.5.4, v2.6.2.3, or v2.7.1.3 and you are indexing an Interplay Production or Interplay Archive database, you must stop the PEBCo agent in the Interplay Administrator.

   For more information, see "Stopping and Starting the PEBCo Agent" on page 64.

6. Start the installation script:

   `./install.sh`

Be sure to use the dot-slash ("./") notation, which tells Linux to look for the installation script in the current directory. Otherwise you will receive the following error message:

```
-bash: install.sh: command not found
```

If you are upgrading from MCS v2.2.x or v2.3.x and your system is configured for Media Index, you will receive a message indicating that "A Media | Index configuration has been detected on this system". Select one of the following options:

- Type **`IGNORE`** if you have already upgraded your Media | Index data or want to upgrade your system without completing the migration.
- Type **`QUIT`** if you have not yet upgraded your Media | Index data and need to exit the installer.

During the installation process, progress is displayed. The update completes with an indication of success:

```
INSTALLATION FINISHED
```

If any errors were encountered during the upgrade, the system reports the following message:

```
INSTALLATION FINISHED WITH ERRORS. Please check the output and log file
/var/log/MediaCentral_Services_<version>_Build_<number>_Linux.log
```

MCS v2.9 and later requires the RHEL OpenSSL security patch to be installed. If this patch was not installed prior to the upgrade, the following message is displayed:

```
A required openssl patch is missing on this system. Please install this
patch (openssl-1.0.1e-30.el6_6.5) so that the system is fully functional.

To check for other missing security fixes execute the avid-security-check
script.
```

If this message is displayed, install the patch now. For details, see the *Avid MediaCentral Platform Services ReadMe*.

7. Verify that the installation was successful using the ics_version script:

   `ics_version`

   Service version numbers are returned as follows:

   ```
   UMS           Version: x.x.x.x
   ICPS          Version: x.x.x.x
   ICPS manager Version: x.x.x.x
   ACS           Version: x.x.x.x
   System ID:    "xxxxxxxxxx"
   ICS installer: 2.10 (Build xx)

   Created on <installer creation date>
   ```

   The ics_version command includes additional information on multi-zone, Media Index, MAM Connector and other components. For precise version numbers, see the *Avid MediaCentral Platform Services 2.10 ReadMe*.

If you receive a "command not found" error, logout and log back into the server or SSH session (PuTTY). This refreshes the login for the upgraded system and should allow the command to run properly.

8. Unmount the USB drive.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

Continuing the Upgrade

Review and complete the steps in this section as they apply to your environment.

To continue the upgrade:

1. In some cases, the installer alerts the user to the creation of .rpmnew files when it encounters a configuration file with custom modifications. In other cases, the system administrator must manually check for updated configuration files.

   Review "Verifying System Configuration Files" on page 65 to check for and update any modified configuration files.

2. (Multi-Zone configurations only) If you are upgrading from MCS v2.3.x or earlier, once the master zone has been updated, run the following script from the master zone to re-enable the database syncing between all zones:

   `/opt/avid/cluster/bin/pgpool_remote_start`

   This step is not required and should not be completed if upgrading from MCS v2.4 or later.

3. If you are connecting to either an Avid ISIS or Avid NEXIS shared storage system, verify the shared storage client required for your environment and upgrade the client software if necessary. For more information, see "Upgrading the Avid Shared Storage Client" on page 14.

4. If additional components (e.g. Closed Captioning Service, MAM Connector, etc.) require updating, complete those upgrades at this time.

   For upgrade instructions for each of these components, see the *MediaCentral Platform Services Installation and Configuration Guide*.

Failure to upgrade previously installed components may result in unexpected errors when testing the system. Make sure you upgrade any previously installed add-in components or uninstall the components if they are no longer used.

5. (Media Index configurations only) Depending upon your upgrade path, additional steps are required to complete the installation. Review the following:

   If you upgraded from MCS v2.4.x, v2.5.x, v2.6.x, or 2.7x, a migration script must be run to update the schema to include new features associated with MCS v2.10.

   a. Review the information in Appendix E for Verifying the Media Index Status to ensure that no active schema migration is currently affecting Media Index.

   b. Once you have verified the status, type the following to run the migration script:

      `/opt/avid/media-index/avid-acs-media-index-migration/avid-acs-media-index-indices-migration`

   If you upgraded from MCS v2.2.x or v2.3.x, a migration script (`media-index-upgrade.sh`) was run prior to the upgrade. However, a second migration script (`avid-acs-media-index-indices-migration`) must now be run to complete the process.

   a. Review the information in Appendix E for Verifying the Media Index Status to ensure that no active schema migration is currently affecting Media Index.

   b. Once you have verified the status, type the following to run the migration script:

      `/opt/avid/media-index/avid-acs-media-index-migration/avid-acs-media-index-indices-migration`

   If you upgraded from MCS v2.1.x or earlier, the Media Index configuration was reset and a data migration is not required. However, the Media Index configuration must be reconfigured at this time.

   For instructions on reconfiguring Media Index, see "Upgrading Media Index from v2.0.x or v2.1.x" the *Avid Media | Index Configuration Guide*.

   If you upgraded from a version of MCS prior to v2.3.2.5, v2.4.2.4, v2.5.4, v2.6.2.3, or v2.7.1.3 and you stopped the PEBCo agent prior to the upgrade, you must restart the PEBCo agent in the Interplay Administrator.

   For more information, see "Stopping and Starting the PEBCo Agent" on page 64.

6. (Media Index configurations only) Systems configured with Media Index for MAM that have upgraded from MCS v2.4.x or v2.5.x must re-sync the legal list using the MAM CentralSyncAgent to resend dictionary data to the Media Index.

   For more information on using the Interplay MAM Sync Service Administrator, see "Setting Up Interplay | MAM Sync Service" the *Avid Media | Index Configuration Guide* or reference the *Interplay | MAM Sync Service Administrator User's Guide*.

7. MediaCentral Platform Services v2.7 and later requires external systems such as Interplay MAM and Interplay Production that have the Avid Connectivity Toolkit installed to be added to a configuration file on the MCS server.

   For more information, see "Configuring Access for External Systems" in the *MediaCentral Platform Services Installation and Configuration Guide*.

8. (Interplay MAM configurations only) If you are connecting to an Interplay MAM system running v5.6, you must verify the GatewayPort setting in Interplay MAM Control Center.

   For more information, see "Verifying the ACS Gateway Port for Interplay | MAM" on page 47.

9. (Multi-Zone configurations only) If you have upgraded a zone running MCS v2.5 or earlier, reconfigure the multi-zone configuration for sharded Mongo.

   If you are running a multi-zone configuration consisting of zones with mixed software versions, only zones that have been upgraded to MCS v2.6 or later can exist in a sharded Mongo configuration.

   For more information, see "Sharded MongoDB" in the *MediaCentral Platform Services Installation and Configuration Guide*.

10. If you have upgraded from MediaCentral Platform Services v2.6 through v2.8, the sharded Mongo environment must be reconfigured to accommodate the new services included with MCS v2.10.

    - If you are upgrading a single-server in a single-zone environment, enter the following two commands to reconfigure the sharded Mongo configuration:

      `mongo-create-configuration -c`

      `mongo-playbook-setup`

      The `mongo-playbook-setup` command reconfigures the existing sharded Mongo configuration and creates new Mongo services related to the avid-asset and avid-asset-gc services included with MCS v2.9 and later.

    - If you are upgrading a multi-zone environment, enter the following two commands on the sharded Mongo "management node" in the master zone to reconfigure the sharded Mongo configuration

      `mongo-create-configuration -c`

      `mongo-playbook-setup`

      Once a slave zone has been upgraded, you must return to the management node in the master zone and run the above two commands again. This will reconfigure the environment once again to enable the services on the remote zones. This process also creates any sharded Mongo arbiters required for the sharded Mongo deployment for avid-asset.

The sharded Mongo configuration scripts included with MCS v2.10 know not to configure sharded Mongo for the avid-asset service on any zones that are not already running MCS v2.9 or later.

The sharded Mongo "management node" is often the master node of a master zone. Users can verify the node by reviewing the contents of the ansible hosts file at: /opt/avid/installer/ansible/hosts. The management node's hostname is identified as "node0" in this file.

For more information on each of these commands, including example output of the commands and troubleshooting, see the "Sharded MongoDB" chapter of the *MediaCentral Platform Services Installation and Configuration Guide*.

11. Once the upgrade is complete, you should verify basic functionality. For more information, see "Verifying the Installation" in the *MediaCentral Platform Services Installation and Configuration Guide*.

    If you experience any issues that you suspect could be related to the browser, see "Clearing the Browser Cache" on page 50 for assistance.

Upgrading a RHEL 6.5 Cluster System to MCS v2.10

Installing MCS v2.10 on a cluster already operating under RHEL v6.5 involves an automated update of the affected packages. All MCS system settings are preserved. All nodes must be taken offline to perform the update.

The cluster upgrade involves the following steps:

- Identifying the Master, Slave and Load-Balancing Nodes
- Backing-up the User Database and System Settings
- Additional Steps for Systems with Media Index
- Taking the Cluster Offline
- Updating the Cluster
- Stopping the RabbitMQ Service and Rebooting the Cluster
- Verifying the RabbitMQ Cluster
- Bringing the Corosync Cluster Online
- Continuing the Upgrade
- (if applicable) Verifying Gluster Volume Permissions
- (if applicable) Removing the Gluster Metadata Cache Replication Volume

Estimated downtime: 2 hours for two servers. 30 minutes - 1 hour for each additional server.

Prior to upgrading, ensure you have verified the "Upgrade Prerequisites" on page 17.

As a reminder, MCS v2.6.0 and later requires sharded Mongo to be configured on all systems configured in a Corosync cluster or a multi-zone configuration. The process for configuring sharded Mongo is referenced in the upgrade process below.

Identifying the Master, Slave and Load-Balancing Nodes

There are three types of nodes in a cluster: master, slave, and load-balancing. The master "owns" multiple resources such as the cluster IP address. The slave assumes the role of master in the event of a fail-over. Additional nodes play a load-balancing role, but can never take on the role of master.

To identify the cluster nodes:

1. Verify the current role of each node in the cluster through the Cluster Resource Monitor. Log in to any machine in the cluster as the root user and type:

   `crm_mon`

2. To identify the master and slave nodes, look for the line containing "Master/Slave Set".

   For example:

   ```
   Master/Slave Set: ms_drbd_postgres [drbd_postgres]
   Masters: [ wavd-mcs01 ]
   Slaves: [ wavd-mcs02 ]
   ```

   In this example, the master node is *wavd-mcs01* and the slave node is *wavd-mcs02*.

3. To identify the load-balancing nodes, look for the line containing “Clone Set”.

   For example:

   ```
   Clone Set: AvidAllEverywhere [AvidAll]
   Started: [ wavd-mcs01 wavd-mcs02 wavd-mcs03 wavd-mcs04]
   ```

   In this example, the load-balancing nodes are *wavd-mcs03* and *wavd-mcs04*.

4. Exit crm_mon by pressing CTRL-C on the keyboard.

Backing-up the User Database and System Settings

Although the upgrade is non-destructive, it is a good idea to back-up the MCS database. This is an optional, but recommended step.

To back up the database and settings:

1. Prepare the v2.10 MCS Installation USB Drive and connect it to the cluster master node.

   For details, see “Creating the MCS Installation USB Drive” in the *MediaCentral Platform Services Installation and Configuration Guide*.

2. Mount the USB drive and change to the mount point.

   For details, see “Mounting and Unmounting a USB Drive” on page 51.

3. Back up the current system settings and MCS database using the backup script.

   For additional detail on using this script, see “Backing Up and Restoring System Settings and the ICS/MCS Database” on page 67.

4. Repeat this process for the slave node and all load balancing nodes.

Additional Steps for Systems with Media Index

If you are upgrading from a version of MCS prior to v2.3.2.5, v2.4.2.4, v2.5.4, v2.6.2.3, or v2.7.1.3 and you are indexing an Interplay Production or Interplay Archive database, you must stop the PEBCo agent in the Interplay Administrator before upgrading the software.

For more information, see “Stopping and Starting the PEBCo Agent” on page 64.

If you are upgrading from MCS v2.2.x or v2.3.x, you need to run a schema migration script prior to upgrading the MCS software. The script can be run from any cluster node and must be run while the cluster is online.

To run the Media Index migration script:

1. Review the information in Appendix E for Verifying the Media Index Status to ensure that no active schema migration is currently affecting Media Index.
2. Once you have verified the status, run the migration script from the root of the MCS Installation USB Drive:

   `./media-index-upgrade.sh`

   This script will update the indexes to be compatible with the MCS v2.10 index structure.

The elasticsearchEverywhere cluster resource must be running for this script to complete the migration tasks.

Taking the Cluster Offline

Corosync and RabbitMQ maintain independent clustering mechanisms. Corosync clusters operate in a master/slave relationship whereas RabbitMQ clusters run in an Active/Active state where any node in the cluster could be the owner of a RabbitMQ "queue". This means that the order in which the nodes disconnect and reconnect to the RabbitMQ cluster is particularly important.

Take care to note the order in which nodes are taken offline. The node that is "last down" must be the node that is "first up". Failure to do so may break the RabbitMQ cluster.

In the following process, each node of the Corosync cluster is put into "standby" and the RabbitMQ service is stopped to pause its clustering functionality. Complete this process one node at a time, waiting 30 seconds between each node. Avid recommends starting with the final node first.

To bring the cluster into standby mode:

1. Begin by putting the Corosync load-balancing nodes into standby mode and stopping the rabbitmq service. Complete this process one node at a time, waiting 30 seconds between each node:

   `crm node standby <node name>`

   `service rabbitmq-server stop`

   Verify that the stop command returns a value of [OK]. If the service does not stop correctly, troubleshoot the issue before continuing.

2. Wait 30 seconds and put the Corosync slave node into standby:

   `crm node standby <node name>`

   `service rabbitmq-server stop`

   Verify that the stop command returns a value of [OK]. If the service does not stop correctly, troubleshoot the issue before continuing.

3. Wait 30 seconds and put the Corosync master node into standby:

   `crm node standby <node name>`

   `service rabbitmq-server stop`

   Verify that the stop command returns a value of [OK]. If the service does not stop correctly, troubleshoot the issue before continuing.

Updating the Cluster

Upgrade the nodes in the reverse order that you stopped the services. Start with the Corosync master node, followed by the slave node and finally the load balancing nodes.

To update the cluster:

1. If you have not already done so, prepare the v2.10 MCS Installation USB Drive and connect it to your first MCS server.

   It is necessary to upgrade the system using the MCS Installation USB Drive as it contains the RHEL v6.5 ISO required for the upgrade process.

   For details, see "Creating the MCS Installation USB Drive" in the *MediaCentral Platform Services Installation and Configuration Guide*.

2. Mount the USB drive and change to the mount point.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

3. Start the installation script.

   `./install.sh`

Be sure to use the dot-slash ("./") notation, which tells Linux to look for the installation script in the current directory. Otherwise you will receive the following error message:

```
-bash: install.sh: command not found
```

If you are upgrading from MCS v2.2 or v2.3 and your system is configured for Media Index, you will receive a message indicating that "A Media | Index configuration has been detected on this system". Select one of the following options:

- Type **`IGNORE`** if you have already upgraded your Media | Index data or want to upgrade your system without completing the migration.
- Type **`QUIT`** if you have not yet upgraded your Media | Index data and need to exit the installer.

During the installation process, progress is displayed. The update completes with an indication of success:

```
INSTALLATION FINISHED
```

If any errors were encountered during the upgrade, the system reports the following message:

```
INSTALLATION FINISHED WITH ERRORS. Please check the output and log file
/var/log/MediaCentral_Services_<version>_Build_<number>_Linux.log
```

MCS v2.9 and later requires the RHEL OpenSSL security patch to be installed. If this patch was not installed prior to the upgrade, the following message is displayed:

```
A required openssl patch is missing on this system. Please install this
patch (openssl-1.0.1e-30.el6_6.5) so that the system is fully functional.

To check for other missing security fixes execute the avid-security-check
script.
```

If this message is displayed, install the patch now. For details, see the *Avid MediaCentral Platform Services ReadMe*.

4. Verify that the installation was successful using the ics_version script:

   `ics_version`

   Service version numbers are returned as follows:

```
UMS           Version: x.x.x.x
ICPS          Version: x.x.x.x
ICPS manager Version: x.x.x.x
ACS           Version: x.x.x.x
System ID:    "xxxxxxxxxxx"

ICS installer: 2.10 (Build xx)
Created on <installer creation date>
```

   The ics_version command includes additional information on multi-zone, Media Index, MAM Connector and other components. For precise version numbers, see the *Avid MediaCentral Platform Services 2.10 ReadMe*.

If you receive a "command not found" error, logout and log back into the server or SSH session (PuTTY). This refreshes the login for the upgraded system and should allow the command to run properly.

5. In some cases, the installer alerts the user to the creation of .rpmnew files when it encounters a configuration file with custom modifications. In other cases, the system administrator must manually check for updated configuration files.

   Review "Verifying System Configuration Files" on page 65 to check for and update any modified configuration files.

6. Unmount the USB drive, proceed to the next node, and follow the same pattern:
   a. Mount the MCS v2.10 Installation USB drive
   b. Run the update script
   c. Verify the ics_version output
   d. Check for configuration file updates
   e. Unmount the USB drive
7. If your system is already configured with the Closed Captioning Service, Maestro UX Plug-In, or the MAM Connector, upgrade those components at this time.

   For upgrade instructions for each of these components, see the *MediaCentral Platform Services Installation and Configuration Guide*.

Failure to upgrade previously installed components may result in unexpected errors when testing the system. Make sure you upgrade any previously installed add-in components or uninstall the components if they are no longer used.

Stopping the RabbitMQ Service and Rebooting the Cluster

During the MCS installation process, the RabbitMQ service is restarted automatically. Depending on your upgrade path, the service might need to be stopped and the servers rebooted.

- If you are upgrading from MCS v2.2.3 or earlier, this process is required.
- If you are upgrading from MCS v2.2.4 or later, this process can be skipped.

To stop RabbitMQ and reboot the cluster:

1. Stop the RabbitMQ services on the final load-balancing node:

   ```
   service rabbitmq-server stop
   ```

   Example: If you have four cluster nodes, number 4 is the "final" load-balancing node.

2. Waiting 30 seconds between each node, stop the RabbitMQ services on the next load-balancing node, then the slave node and finally the master node.

   Verify that the stop command returns a value of [OK]. If the service does not stop correctly, troubleshoot the issue before continuing.

3. Once the RabbitMQ services have been stopped on each node, all nodes in the cluster must be rebooted. The order in which the nodes are rebooted is important to ensure RabbitMQ starts successfully. Begin by rebooting the master node:

   ```
   reboot
   ```

4. Waiting 30 seconds between each node, reboot the slave node and each load-balancing node.

   ```
   reboot
   ```

5. Once all nodes have been rebooted and RabbitMQ has been started on each node, verify the status of the RabbitMQ cluster as detailed in the following process.

Verifying the RabbitMQ Cluster

Prior to restoring the Cosrosync cluster, you should first verify that the RabbitMQ cluster is functioning normally. Complete the following two steps on each cluster node.

To verify the status of RabbitMQ:

1. Verify the status of the RabbitMQ service:

   `service rabbitmq-server status`

   The command will return a detailed string of data regarding the service. Example (partial only):

   ```
   [root@mcs-1 ~]# service rabbitmq-server status
   Status of node 'rabbit@mcs-1' ...
   [{pid,2064},
    {running_applications,
       [{rabbitmq_federation_management,"RabbitMQ Federation
   Management","3.3.5"},
        {rabbitmq_management,"RabbitMQ Management Console","3.3.5"},
   ```

   Review the output of the command and verify there are no obvious error messages such as "`service is dead but pid (xxxxx) is running`".

2. Check the RabbitMQ cluster with the "rabbitmqctl cluster_status" command:

   `rabbitmqctl cluster_status`

   The following is an example of a 2-node cluster:

   ```
   Cluster status of node 'rabbit@node-n1' ...
   [{nodes,[{disc,['rabbit@node-n1','rabbit@node-n2']}]},
   {running_nodes,[ 'rabbit@node-n1','rabbit@node-n2']},
   {cluster_name,<<"rabbit@node-n1">>},
   {partitions,[]}]
   ```

   The command should return information about each of the RabbitMQ cluster nodes. All available nodes should appear on both the "nodes" and "running_nodes" lines.

   Verify that each node reports the same information about the RabbitMQ cluster (all nodes are known and running).

The RabbitMQ cluster must be healthy prior to bringing the Corosync cluster back online. If you suspect there is a problem, see the following Avid Knowledge Base article for assistance:

http://avid.force.com/pkb/articles/en_US/troubleshooting/RabbitMQ-cluster-troubleshooting

Bringing the Corosync Cluster Online

The next step in the process is to bring the Cosrosync cluster back online and verify that the cluster is functioning normally.

To bring the cluster back online:

1. Reactivate the cluster by running the following command on the master node only:

   `/opt/avid/cluster/bin/reactivate-cluster`

   The script will begin collecting information about your system.

2. The script creates a backup copy of the cluster configuration file. If you have previously upgraded your MCS server, a configuration backup file already exists. You are asked to confirm that you want to overwrite this backup file:

   ```
   File /root/ics_cluster_config_reinit.bak exists. Do you want to overwrite
   it (y/n)?
   ```

   Enter "**y**" to proceed.

3. A list of configuration settings appears on the screen. You are asked to confirm these settings:

   ```
   Do you wish to apply these settings? y/n
   ```

   If the information is correct, enter "**y**" to proceed.

   Be patient as the script brings all nodes back online.

4. Start the Cluster Resource Monitor to verify the cluster status:

   crm_mon -f

   - Verify the master, slave, and load-balancing nodes (if applicable) are online.
   - Review the fail counts for the cluster resources.

If after running the reactivate-cluster script you observe that a node is the state of "Offline - Unclean Node", restart the Pacemaker service on that node.

If the reactivate-cluster command does not bring all nodes back online, you can complete the process manually. For example, to bring the master node back online:

crm node online *<node name>*

Wait 30 seconds and bring the slave node back online:

crm node online *<node name>*

If applicable, bring the load-balancing nodes back online:

crm node online *<node name>*

5. You should see failures in the Cluster Resource Monitor related to the AvidAsset resource. This is normal since you have not yet reconfigured sharded Mongo. The process for reconfiguring sharded Mongo for the avid-asset services is covered in "Continuing the Upgrade" on page 31.

   If the Cluster Resource Monitor shows resource failures, run the Cluster Resource Manager cleanup command to reset them:

   crm resource cleanup *<rsc>* [*<node>*]

   <rsc> is the resource name of interest: AvidIPC, pgsqlDB (or another)

   <node> (optional) is the node of interest

If you receive an "object/attribute does not exist" error message, it indicates the resource is active on more than one node. Repeat the command using the "everywhere" form of the resource.

For example, to reset the fail count for AvidAll resource, issue the following command:

crm resource cleanup AvidAllEverywhere

You can address the services contained in the postgres resource group (postgres_fs, AvidClusterIP and pgsqlDB) individually, or as a group.

Continuing the Upgrade

Review and complete the steps in this section as they apply to your environment.

To continue the upgrade:

1. (Multi-Zone configurations only) If you are upgrading from MCS v2.3.x or earlier, once the master zone has been updated, run the following script from the Master node of the cluster in the Master zone to re-enable the database syncing between all zones.

   `/opt/avid/cluster/bin/pgpool_remote_start`

   This step is not required and should not be completed if upgrading from MCS v2.4 or later.

2. If you are connecting to either an Avid ISIS or Avid NEXIS shared storage system, verify the shared storage client required for your environment and upgrade the client software if necessary. For more information, see "Upgrading the Avid Shared Storage Client" on page 14.

3. (Media Index configurations only) Depending upon your upgrade path, additional steps are required to complete the installation. Review the following:

   If you upgraded from MCS v2.4.x, v2.5.x, v2.6.x, or 2.7.x, a migration script must be run to update the schema to include new features associated with MCS v2.10.

   a. Review the information in Appendix E for Verifying the Media Index Status to ensure that no active schema migration is currently affecting Media Index.

   b. Once you have verified the status, type the following to run the migration script:

      `/opt/avid/media-index/avid-acs-media-index-migration/avid-acs-media-index-indices-migration`

   If you upgraded from MCS v2.2.x or v2.3.x, a migration script (`media-index-upgrade.sh`) was run prior to the upgrade. However, a second migration script (`avid-acs-media-index-indices-migration`) must now be run to complete the process.

   a. Review the information in Appendix E for Verifying the Media Index Status to ensure that no active schema migration is currently affecting Media Index.

   b. Once you have verified the status, type the following to run the migration script:

      `/opt/avid/media-index/avid-acs-media-index-migration/avid-acs-media-index-indices-migration`

   If you upgraded from MCS v2.1.x or earlier, the Media Index configuration was reset and a data migration is not required. However, the Media Index configuration must be reconfigured at this time.

   For instructions on reconfiguring Media Index, see "Upgrading Media Index from v2.0.x or v2.1.x" the *Avid Media | Index Configuration Guide*.

   If you upgraded from a version of MCS prior to v2.3.2.5, v2.4.2.4, v2.5.4, v2.6.2.3, or v2.7.1.3 and you stopped the PEBCo agent prior to the upgrade, you must restart the PEBCo agent in the Interplay Administrator.

   For more information, see "Stopping and Starting the PEBCo Agent" on page 64.

4. (Media Index configurations only) Systems configured with Media Index for MAM that have upgraded from MCS v2.4.x or v2.5.x must re-sync the legal list using the MAM CentralSyncAgent to resend dictionary data to the Media Index.

   For more information on using the Interplay MAM Sync Service Administrator, see "Setting Up Interplay | MAM Sync Service" the *Avid Media | Index Configuration Guide* or reference the *Interplay | MAM Sync Service Administrator User's Guide*.

5. MediaCentral Platform Services v2.7 and later requires external systems such as Interplay MAM and Interplay Production that have the Avid Connectivity Toolkit installed to be added to a configuration file on the MCS server.

   For more information, see "Configuring Access for External Systems" in the *MediaCentral Platform Services Installation and Configuration Guide*.

6. (Interplay MAM configurations only) If you are connecting to an Interplay MAM system running v5.6, you must verify the GatewayPort setting in Interplay MAM Control Center.

   For more information, see "Verifying the ACS Gateway Port for Interplay | MAM" on page 47.

7. If you have upgraded from MCS v2.5 or earlier, reconfigure the configuration for sharded Mongo. This step is required for all Corosync cluster configurations that have upgraded from v2.5 or earlier.

   For more information, see "Sharded MongoDB" in the *MediaCentral Platform Services Installation and Configuration Guide.*

If you are running a multi-zone configuration consisting of zones with mixed software versions, only zones that have been upgraded to MCS v2.6 or later can exist in a sharded Mongo configuration.

8. If you have upgraded from MediaCentral Platform Services v2.6 through v2.8, the sharded Mongo environment must be reconfigured to accommodate the new services included with MCS v2.10.

   - If you are upgrading a single-zone cluster, enter the following two commands on the sharded Mongo "management node" to reconfigure the sharded Mongo configuration:

     `mongo-create-configuration -c`

     `mongo-playbook-setup`

     The `mongo-playbook-setup` command reconfigures the existing sharded Mongo configuration and creates new Mongo services related to the avid-asset and avid-asset-gc services included with MCS v2.9 and later.

   - If you are upgrading a multi-zone environment, enter the following two commands on the sharded Mongo "management node" in the master zone to reconfigure the sharded Mongo configuration

     `mongo-create-configuration -c`

     `mongo-playbook-setup`

     After upgrading a slave zone, you must return to the management node in the master zone and run the above commands again. This will reconfigure the environment once again to enable the services on the remote zones. This process also creates any sharded Mongo arbiters required for the sharded Mongo deployment for avid-asset.

The sharded Mongo configuration scripts included with MCS v2.10 know not to configure sharded Mongo for the avid-asset service on any zones that are not already running MCS v2.9 or later.

The sharded Mongo "management node" is often the master node of a master zone. Users can verify the node by reviewing the contents of the ansible hosts file at: /opt/avid/installer/ansible/hosts. The management node's hostname is identified as "node0" in this file.

For more information on each of these commands, including example output of the commands and troubleshooting, see the "Sharded MongoDB" chapter of the *MediaCentral Platform Services Installation and Configuration Guide*.

9. If your system includes Media Distribute or the Assignments Pane, upgrade those software components at this time.

   For upgrade instructions for each of these components, see the *MediaCentral Platform Services Installation and Configuration Guide*.

10. Once the upgrade is complete, you should verify basic functionality. For more information, see "Verifying the Installation" in the *MediaCentral Platform Services Installation and Configuration Guide*.

    If you experience any issues that you suspect could be related to the browser, see "Clearing the Browser Cache" on page 50 for assistance.

(if applicable) Verifying Gluster Volume Permissions

The process below was added to the v2.2.0 *MediaCentral Platform Services Installation and Configuration Guide*. Depending on when your system was installed, permissions for some Gluster volumes may or may not have been set correctly. If you have upgraded from a system running MCS v1.8.1, MCS v2.0.x or MCS v2.1.x, complete the following procedure. If you have upgraded from MCS v2.2 or later, this process should have already been completed and is not required.

The following directories must be owned by user maxmin and have group id set to maxmin:

`cache/gluster/gluster_data_download`

`cache/gluster/gluster_data_fl_cache`

These directories are associated with RHEL directories (`/cache/download` and `/cache/fl_cache`) used to store files for http-based streaming, such as media converted to FLV for file-based playback. They are also used to store media converted to Mpeg2TS for playback on iOS devices. The `download` directory contains links to simplify iOS playback.

Restarting the Gluster daemon (glusterd) results in user ID and group ownership of the Gluster volumes being changed from maxmin to root, which breaks playback on iOS devices. Thus if a cluster node is rebooted, playback issues can arise.

To prevent issues for an existing cluster, you must configure the two Gluster cache volumes to use the same UID and GID as the maxmin user, as described in the following procedure.

On each node in the cluster perform the following steps (all nodes, one at a time in any order).

To set Gluster volume ownership so it does not change:

1. Obtain the user ID (uid) of the user maxmin (this might be different on each machine):

   `id -u maxmin`

2. Change the user ownership of the Gluster volume to maxmin using the user ID:

   `gluster volume set gl-cache-dl storage.owner-uid <uid>`

   `gluster volume set gl-cache-fl storage.owner-uid <uid>`

   In the above commands, do not type the angle brackets. Enter the number obtained in the previous step.

Do not alter the gl-cache-mcam (multicam) volume. It uses the default root ownership.

3. Obtain the group ID (gid) of the user maxmin (this might be different on each machine):

   id -g maxmin

4. Change the group ownership of the gluster volume to maxmin using the group ID:

   gluster volume set gl-cache-dl storage.owner-gid <*gid*>

   gluster volume set gl-cache-fl storage.owner-gid <*gid*>

Do not alter the gl-cache-mcam (multicam) volume. It uses the default root ownership.

5. Verify the success of the ownership changes:

   ls -la /cache/gluster

   Should return:

   ```
   drwxrwsrwx 3 maxmin maxmin 4096 Jan 12 09:51 gluster_data_download
   drwxrwsrwx 5 maxmin maxmin 4096 Jan 12 09:51 gluster_data_fl_cache
   drwxr-xr-x 3 root   root   4096 Feb  5 08:33 gluster_data_multicam
   ```

6. Restart the GlusterFS service:

   service glusterd restart

7. Once the service has been restarted, verify that the ownership changes have been maintained:

   ls -la /cache/gluster

   This command should return same values as seen in step 5:

   ```
   drwxrwsrwx 3 maxmin maxmin 4096 Jan 12 09:51 gluster_data_download
   drwxrwsrwx 5 maxmin maxmin 4096 Jan 12 09:51 gluster_data_fl_cache
   drwxr-xr-x 3 root   root   4096 Feb  5 08:33 gluster_data_multicam
   ```

8. Using the `chown` command, change the ownership of any files residing in the `gluster_data_download` and `gluster_data_fl_cache` directories:

   chown -R maxmin:maxmin /cache/gluster/gluster_data_download

   chown -R maxmin:maxmin /cache/gluster/gluster_data_fl_cache

(if applicable) Removing the Gluster Metadata Cache Replication Volume

If you are upgrading from MCS v2.0, additional configuration steps might be required. Early versions of the *MediaCentral Platform Services v2.0 Installation and Configuration Guide* instructed users to create a Gluster replicated “metadata” directory for Interplay | MAM deployments.

The use of Gluster to replicate metadata has been deprecated due to its negative impact on performance. If this directory exists, it must be removed from all server nodes. Once the directory has been deleted, metadata information is loaded into RAM and is no longer replicated across the nodes.

For instructions, consult the Avid KB article “Removing the GlusterFS Metadata Cache Replication Volume” at the following link:

http://avid.force.com/pkb/articles/en_US/how_to/Removing-the-gluster-metadata-cache-replication-volume

3 Upgrades for RHEL v6.3 Systems

If upgrading a MediaCentral Platform Services system running RHEL v6.3, refer to one of the following two processes:

- Upgrading a RHEL 6.3 Single Server to MCS v2.10
- Upgrading a RHEL 6.3 Cluster System to MCS v2.10

Before proceeding, back up any private key used to generate a Certificate Signing Request. For details, see "Backing Up and Restoring SSL Private Keys" on page 16.

Upgrading a RHEL 6.3 Single Server to MCS v2.10

The upgrade to MCS v2.10 on a RHEL v6.3 system involves a fresh installation of the operating system and of MediaCentral Platform Services. This process consists of the following procedures:

- Backing-up System Settings
- Installing RHEL 6.5 and MCS 2.10
- Restoring System Settings and Migrating the User Database
- Additional Upgrade Procedures

Estimated downtime: 3 hours

Backing-up System Settings

As this upgrade requires a re-image of the MCS server, a manual backup of the system settings is critical to the success of the upgrade.

To back up the system settings:

1. Prepare the v2.10 MCS Installation USB Drive and connect it to your MCS server.

   For details, see "Creating the MCS Installation USB Drive" in the *MediaCentral Platform Services Installation and Configuration Guide*.

2. Mount the USB drive and change to the mount point.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

The MCS Installation USB Drive contains all software used to image a new MediaCentral server. Do not reboot the server with this USB drive attached!

3. Back up the current system settings and ICS/MCS database using the backup script.

   For additional detail on using this script, see "Backing Up and Restoring System Settings and the ICS/MCS Database" on page 67.

4. Unmount and remove the USB drive.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

Installing RHEL 6.5 and MCS 2.10

Once the system settings have been backed-up and stored in a safe location, the MCS server can be re-imaged with a fresh installation of RHEL v6.5 and MediaCentral Platform Services.

To install RHEL v6.5 and MCS:

1. Unmount the USB drive (if you have not already done so).

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

2. If your configuration includes a RAID 5 array, delete and recreate the RAID 5. Destroying and re-creating the RAID 5 eliminates (in advance) any problems with cache permissions that can arise as a result of the RHEL update.

   For details on deleting the RAID 5, see "Deleting the RAID 5 Array" on page 55.

   For details on recreating the RAID 5, see "Configuring the Onboard RAID" in the *MediaCentral Platform Services Installation and Configuration Guide*.

3. Insert the USB drive and boot from it to install RHEL and MCS.

   For details, see "Installing RHEL and the MCS Software" in the *MediaCentral Platform Services Installation and Configuration Guide*.

4. Once installed, remove the USB drive and reboot as prompted.

   Rebooting after the OS upgrade causes the RHEL Text Mode Setup Utility ("Choose a Tool" screen) to appear, providing access to set-up menus.

5. Quit the RHEL Text Mode Setup Utility and log in to the RHEL console.

6. Verify that the installation was successful using the ics_version script:

   `ics_version`

   Service version numbers are returned as follows:

   ```
   UMS           Version: x.x.x.x
   ICPS          Version: x.x.x.x
   ICPS manager  Version: x.x.x.x
   ACS           Version: x.x.x.x
   System ID:    "xxxxxxxxxxx"

   ICS installer: 2.10 (Build xx)
   Created on <installer creation date>
   ```

   The ics_version command includes additional information on multi-zone, Media Index, MAM Connector and other components. For precise version numbers, see the *Avid MediaCentral Platform Services v2.10 ReadMe*.

If you receive a "command not found" error, logout and log back into the server or SSH session (PuTTY). This will refresh the login for the upgraded system.

7. Install any RHEL security updates.

   For details, see the *Avid MediaCentral Platform Services v2.10 ReadMe*.

Restoring System Settings and Migrating the User Database

Now that RHEL v6.5 and MediaCentral Platform Services has been installed on the server, the custom MCS settings must be restored from the USB backup.

To restore the MCS settings:

1. Re-insert and re-mount the USB drive.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

The MCS Installation USB Drive contains all software used to image a new MediaCentral server. Do not reboot the server with this USB drive attached!

2. Restore the system settings and MCS database using the restore script.

   For additional detail on using this script, see "Backing Up and Restoring System Settings and the ICS/MCS Database" on page 67.

   During the restore process, error messages similar to the following might be displayed:

   ```
   /usr/maxt/maxedit/cluster/resources/_common.sh errors
   ```

   If this occurs, ignore the messages, type the following, and press Enter to complete the command:

   `service avid-all stop`

You do not need to stop the error messages to type the above command. You can enter the command even as the error messages are output to the terminal.

3. Unmount and remove the USB drive.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

4. Reboot and note the restored host name at the login prompt (e.g. wavd-mcs01).

   If you see the original host name at the login prompt, it signifies that the system settings were successfully restored.

5. Log in as the root user and migrate the user settings from the UMS database to the USS database (new in MCS v2.0):

   `/opt/avid/bin/avid-uss-import`

   The system returns the following:

   ```
   Loading properties..
   Fetching zone UUID..
   Importing settings for zone UUID: 00000000-0000-0000-0000-000000000000
   Importing setting_domain_class..
   Importing setting_class..
   Importing setting_instance..
   SUCCESS
   ```

Additional Upgrade Procedures

The backup and restore procedure saves many system settings which provides the user with a more streamlined upgrade. However, some configuration steps must be manually recreated. Refer to the appropriate section of the *MediaCentral Platform Services Installation and Configuration Guide* for details on each of the following procedures.

To complete the upgrade:

1. If your configuration includes a RAID 5, recreate the file cache. See "Creating the File Cache on the RAID".
2. Verify the contents of the hosts file. See "Verifying the hosts File Contents".
3. MediaCentral Platform Services v2.7 and later requires external systems such as Interplay Production and Interplay MAM that have the Avid Connectivity Toolkit installed to be added to a configuration file on the MCS server.

   For more information, see "Configuring Access for External Systems" in the *MediaCentral Platform Services Installation and Configuration Guide*.
4. Verify the date and time settings. See "Configuring Date and Time Settings".
   a. Though time zone information was restored, you must re-create the symbolic link RHEL needs to make use of it:

      `ln -sf /usr/share/zoneinfo/<yourzone> /etc/localtime`

      If you need to verify the zone in use prior to re-creating the symbolic link:

      `cat /etc/sysconfig/clock`

   b. Verify the availability of the in-house NTP server, synchronize the system clock, and set up a cron job to keep the clock synchronized.
5. Compare the current (active) and restored file system table files "fstab" for changes:

   `cat /<path>/fstab`

   - The current "live" file system table is located at: `/etc/fstab`
   - The restored file system table is located at: `/root/fstab`

   Since some entries in the file are assigned UUIDs dynamically by Linux, the restore script does not place the `fstab` file in its original location. These UUIDs can change from one RHEL installation to the next, even if they underlying hardware remains the same. Therefore it is important to manually compare the contents of the restored file to the original file to ensure all system settings are migrated.

   For example, in an MCS system configured for Interplay | MAM, the fstab file contains an entry to automatically mount the Interplay | MAM file system. This information must be manually added to the active file at: `/etc/fstab`

   Add information to the "live" fstab file as necessary.

The UUID information will be different between "live" and restored fstab files. Do not alter this information.

6. If you are deploying MCS for Interplay | MAM or Media Composer | Cloud, you must update MediaCentral configuration settings.

   For details, see "Reconfiguring MCS for Upgrades from ICS v1.7 or Earlier" on page 47.

7. If you are connecting to either an Avid ISIS or Avid NEXIS shared storage system, verify the shared storage client required for your environment and upgrade the client software if necessary. See “Upgrading the Avid Shared Storage Client Software”.
8. Test the system. See the “Verifying the Installation” chapter.

   If you experience any issues that you suspect could be related to the browser, see “Clearing the Browser Cache” on page 50 for assistance.
9. If your workflow includes Closed Captioning, install the MediaCentral UX Closed Captioning Service. See the “Closed Captioning Service” chapter.

The Closed Captioning Service requires the ISIS Virtual Host Name in the MediaCentral UX System Settings (Playback Service) to be entered in all lower case. Verify and update this setting if needed.

10. If your workflow includes additional plug-in services such as the Closed Captioning Service, MAM Connector or others, install and configure the software at this time. See the appropriate chapter in the MCS Install Guide for instructions.
11. (Interplay MAM configurations only) If you are connecting to an Interplay MAM system running v5.6, you must verify the GatewayPort setting in Interplay MAM Control Center.

    For more information, see “Verifying the ACS Gateway Port for Interplay | MAM” on page 47.
12. If your workflow includes Media Distribute, install and configure the software at this time.

    For information on installing Media Distribute, see the M*edia |Distribute Installation and Configuration Guide*, available on the v2.8 Documentation page of the Avid Knowledge Base.
13. If your workflow includes multi-zone or Media Index, configure those items at this time.

    For multi-zone, see the “Multi-Zone” chapter.

    For information on installing Media Index, see the *Avid Media | Index Configuration Guide*.
14. If your workflow includes multi-zone, update the configuration for “sharded” Mongo. See the “Sharded MongoDB” chapter.

    Also review “Upgrading Multi-Zone Deployments” on page 12 for additional information.
15. If you added additional components or made any configuration changes, test the system again. See the “Verifying the Installation” chapter.

    If you experience any issues that you suspect could be related to the browser, see “Clearing the Browser Cache” on page 50 for assistance.
16. Once the system is running to your satisfaction, Avid suggests creating a final backup of the system settings and MCS database.

    For additional detail on using this script, see “Backing Up and Restoring System Settings and the ICS/MCS Database” on page 67.

Upgrading a RHEL 6.3 Cluster System to MCS v2.10

The upgrade to MCS v2.10 on a RHEL v6.3 system involves a fresh installation of the operating system and of MediaCentral Platform Services. This process consists of the following procedures:

- Identifying the Master, Slave and Load-Balancing Nodes
- Backing Up the System Settings
- Taking the Cluster Offline
- Upgrading the Software
- Restoring System Settings and Migrating the User Database
- Additional Upgrade Procedures

Estimated downtime: 4 hours for two servers. 1 hour for each additional server.

Identifying the Master, Slave and Load-Balancing Nodes

There are three types of nodes in a cluster: master, slave, and load-balancing. The master "owns" multiple resources such as the cluster IP address. The slave assumes the role of master in the event of a fail-over. Additional nodes play a load-balancing role, but can never take on the role of master.

To identify the cluster nodes:

1. Verify the current role of each node by logging in to any machine in the cluster as the root user and typing:

   `crm_mon`

2. To identify the master and slave nodes, look for the line containing "Master/Slave Set".

   For example:

   ```
   Master/Slave Set: ms_drbd_postgres [drbd_postgres]
   Masters: [ wavd-mcs01 ]
   Slaves: [ wavd-mcs02 ]
   ```

   In this example, the master node is *wavd-mcs01* and the slave node is *wavd-mcs02*.

3. To identify the load-balancing nodes, look for the line containing "Clone Set".

   For example:

   ```
   Clone Set: AvidAllEverywhere [AvidAll]
   Started: [ wavd-mcs01 wavd-mcs02 wavd-mcs03]
   ```

   In this example, the load-balancing node is *wavd-mcs03*.

4. Exit crm_mon by pressing CTRL-C on the keyboard.

Backing Up the System Settings

As this upgrade requires a re-image of the MCS servers, a manual backup of the system settings is critical to the success of the upgrade.

Ensure that the master node is not in standby when you run the backup script. If it is in standby, only the system settings will be backed up – not the database. All other nodes can be in standby if desired.

To back up the system settings:

1. Prepare the v2.10 MCS Installation USB Drive and connect it to the cluster's master node.

   For details, see "Creating the MCS Installation USB Drive" in the *MediaCentral Platform Services Installation and Configuration Guide*.

2. Mount the USB drive and change to the mount point.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

The MCS Installation USB Drive contains all software used to image a new MediaCentral server. Do not reboot the server with this USB drive attached!

3. Back up the current system settings and ICS/MCS database using the backup script.

   For additional detail on using this script, see "Backing Up and Restoring System Settings and the ICS/MCS Database" on page 67.

   Be sure to create a copy of the backup directory using the Linux cp command. For example:

   ```
   cp -r sys-backup sys-backup-<nodename>
   ```

It is extremely important to copy the backup directory and rename it. Only the master node backup contains the complete system settings and database. If you do not create a copy of the master node backup file, it will be overwritten by the backup from a non-master node and you will lose the database, amongst other information.

4. Unmount the USB drive.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

5. Repeat the above procedure for the slave node and any load-balancing nodes.
6. Before proceeding to the next step, make sure you have a backup file for each node.

Taking the Cluster Offline

Prior to upgrading the cluster, all nodes must be taken offline. To avoid accidental cluster fail-over, make sure to follow the order represented below.

To take the cluster offline:

1. Begin by putting the Corosync load-balancing and slave nodes into standby mode and stopping the rabbitmq service. Complete this process one node at a time, waiting 30 seconds between each node:

   ```
   crm node standby <node name>
   ```

   ```
   service rabbitmq-server stop
   ```

2. Finally, put the Corosync master node into standby mode and stop the rabbitmq service:

   ```
   crm node standby <node name>
   ```

   ```
   service rabbitmq-server stop
   ```

Upgrading the Software

Complete this process for each cluster node (in any order).

To upgrade the software:

1. Unmount the USB drive (if you have not already done so).

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

2. If your configuration includes a RAID 5 array, delete and recreate the RAID 5. Destroying and re-creating the RAID 5 eliminates (in advance) any problems with cache permissions that can arise as a result of the RHEL update.

   For details on deleting the RAID 5, see "Deleting the RAID 5 Array" on page 55.

   For details on recreating the RAID 5, see "Configuring the Onboard RAID" in the *MediaCentral Platform Services Installation and Configuration Guide*.

3. Insert the USB drive and boot from it to install RHEL and MCS.

   For details, see "Installing RHEL and the MCS Software" in the *MediaCentral Platform Services Installation and Configuration Guide*.

4. Once installed, remove the USB drive and reboot as prompted.

   Rebooting after the OS upgrade causes the RHEL Text Mode Setup Utility ("Choose a Tool" screen) to appear, providing access to set-up menus.

5. Quit the RHEL Text Mode Setup Utility and log in to the RHEL console.

6. Verify that the installation was successful using the ics_version script:

   `ics_version`

   Service version numbers are returned as follows:

   ```
   UMS           Version: x.x.x.x
   ICPS          Version: x.x.x.x
   ICPS manager  Version: x.x.x.x
   ACS           Version: x.x.x.x
   System ID:    "xxxxxxxxxxx"

   ICS installer: 2.10 (Build xx)
   Created on <installer creation date>
   ```

   The ics_version command includes additional information on multi-zone, Media Index, MAM Connector and other components. For precise version numbers, see the *Avid MediaCentral Platform Services v2.10 ReadMe*.

If you receive a "command not found" error, logout and log back into the server or SSH session (PuTTY). This will refresh the login for the upgraded system and should allow the command to run properly.

7. Install any RHEL security updates.

   See the *Avid MediaCentral Platform Services v2.10 ReadMe* for more information.

Restoring System Settings and Migrating the User Database

Now that RHEL v6.5 and MediaCentral Platform Services has been installed on the servers, the custom MCS settings must be restored from the USB backup.

To restore the MCS settings:

1. Insert and Mount the USB drive on the master node.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

The MCS Installation USB Drive contains all software used to image a new MediaCentral server. Do not reboot the server with this USB drive attached!

2. Restore the system settings and MCS database using the restore script.

   For additional detail on using this script, see "Backing Up and Restoring System Settings and the ICS/MCS Database" on page 67.

   During the restore process, error messages similar to the following might be displayed:

   ```
   /usr/maxt/maxedit/cluster/resources/_common.sh errors
   ```

   If this occurs, ignore the messages, type the following, and press Enter to complete the command:

   ```
   service avid-all stop
   ```

You do not need to stop the error messages to type the above command. You can enter the command even as the error messages are output to the terminal.

3. Unmount and remove the USB drive.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

4. Verify if DRBD is set to run at system startup:

   ```
   chkconfig --list drbd
   ```

   This command includes two dashes ("--") with no space between them.

5. If set to run, disable DRBD (since it will interfere with setting up the cluster):

   ```
   chkconfig drbd off
   ```

6. Reboot and note the restored host name at the login prompt (e.g. wavd-mcs01).

   If you see the original host name at the login prompt, it signifies that the system settings were successfully restored.

7. (On the Master node only) Log in as the root user and migrate the user settings from the UMS database to the USS database (new in MCS v2.0):

   ```
   /opt/avid/bin/avid-uss-import
   ```

The system returns the following:

```
Loading properties..
Fetching zone UUID..
Importing settings for zone UUID: 00000000-0000-0000-0000-000000000000
Importing setting_domain_class..
Importing setting_class..
Importing setting_instance..
SUCCESS
```

8. Repeat steps 1 through 6 on the slave and load balancing nodes to restore the system settings for each node. Step 7 is completed on the master node only.

Additional Upgrade Procedures

The backup and restore procedure saves many system settings which provides the user with a more streamlined upgrade. However, some configuration steps must be manually recreated. Refer to the appropriate section of the *MediaCentral Platform Services Installation and Configuration Guide* for details on each of the following procedures.

To complete the upgrade:

1. If your configuration includes a RAID 5, recreate the file cache on each cluster node. See "Creating the File Cache on the RAID".
2. Verify the contents of the hosts file. See "Verifying the hosts File Contents".
3. MediaCentral Platform Services v2.7 and later requires external systems such as Interplay Production and Interplay MAM that have the Avid Connectivity Toolkit installed to be added to a configuration file on the MCS server.

   For more information, see "Configuring Access for External Systems" in the *MediaCentral Platform Services Installation and Configuration Guide*.
4. Verify the date and time settings. See "Configuring Date and Time Settings".
   a. Though time zone information was restored, you must re-create the symbolic link RHEL needs to make use of it

      `ln -sf /usr/share/zoneinfo/<yourzone> /etc/localtime`

      If you need to verify the zone in use prior to re-creating the symbolic link:

      `cat /etc/sysconfig/clock`

   b. Verify the availability of the in-house NTP server, synchronize the system clock, and set up a cron job to keep the clock synchronized.
5. Reconfigure the cluster and cache replication. See the "Clustering" chapter.
6. Compare the current and restored file system table files "fstab" for changes:

   `cat /<path>/fstab`

   - The current "live" file system table is located at: `/etc/fstab`
   - The restored file system table is located at: `/root/fstab`

Since some entries in the file are assigned UUIDs dynamically by Linux, the restore script does not place the `fstab` file in its original location. These UUIDs can change from one RHEL installation to the next, even if they underlying hardware remains the same. Therefore it is important to manually compare the contents of the restored file to the original file to ensure all system settings are migrated.

For example, in an MCS system configured for Interplay | MAM, the fstab file contains an entry to automatically mount the Interplay | MAM file system. This information must be manually added to the active file at: `/etc/fstab`

Add information to the "live" fstab file as necessary.

The UUID information will be different between "live" and restored fstab files. Do not alter this information.

7. If you are connecting to either an Avid ISIS or Avid NEXIS shared storage system, verify the shared storage client required for your environment and upgrade the client software if necessary. See "Upgrading the Avid Shared Storage Client Software".
8. Test the cluster. See the "Verifying the Installation" chapter.

   If you experience any issues that you suspect could be related to the browser, see "Clearing the Browser Cache" on page 50 for assistance.
9. If you are deploying MCS for Interplay | MAM or Media Composer | Cloud, you must update MediaCentral configuration settings.

   For details, see "Reconfiguring MCS for Upgrades from ICS v1.7 or Earlier" on page 47.
10. If your workflow includes Closed Captioning, install the MediaCentral UX Closed Captioning Service. See the "Closed Captioning Service" chapter.

The Closed Captioning Service requires the ISIS Virtual Host Name in the MediaCentral UX System Settings (Playback Service) to be entered in all lower case. Verify and update this setting if needed.

11. If your workflow includes additional plug-in services such as the Closed Captioning Service, MAM Connector or others, install and configure the software at this time. See the appropriate chapter in the MCS Install Guide for instructions.
12. (Interplay MAM configurations only) If you are connecting to an Interplay MAM system running v5.6, you must verify the GatewayPort setting in Interplay MAM Control Center.

    For more information, see "Verifying the ACS Gateway Port for Interplay | MAM" on page 47.
13. If your workflow includes Media Distribute, install and configure the software at this time.

    For information on installing Media Distribute, see the M*edia |Distribute Installation and Configuration Guide*, available on the v2.7 Documentation page of the Avid Knowledge Base.
14. If your workflow includes multi-zone or Media Index, configure those items at this time.

    For multi-zone, see the "Multi-Zone" chapter.

    For information on installing Media Index, see the *Avid Media | Index Configuration Guide*.
15. All MediaCentral clusters require sharded Mongo to be configured on the MCS servers. Sharded Mongo is also required for ALL zones in a multi-zone environment. See the "Sharded MongoDB" chapter.

    If running a multi-zone configuration, review "Upgrading Multi-Zone Deployments" on page 12 for additional information.

16. If you added additional components or made any configuration changes, test the system again. See the “Verifying the Installation” chapter.

    If you experience any issues that you suspect could be related to the browser, see “Clearing the Browser Cache” on page 50 for assistance.

17. Once the cluster is running to your satisfaction, Avid suggests creating a final backup of the system settings and MCS database.

    For additional detail on using this script, see “Backing Up and Restoring System Settings and the ICS/MCS Database” on page 67.

A Post Upgrade Notes

The following notes may or may not apply to your configuration.

Configuring MCS System Settings

Updated versions of MediaCentral Platform Services often introduce new features and configuration options. Once the upgrade is complete, system administrators should review the MediaCentral UX System Settings and verify the values for all settings.

For more information, see the "New Features" section of the *MediaCentral Platform Services ReadMe*.

Verifying the ACS Gateway Port for Interplay | MAM

Interplay MAM v5.6 and later includes a "GatewayPort" system setting that specifies the port number used to communicate with the MediaCentral Platform Services avid-acs-gateway service. All Interplay MAM servers hosting services that use the new Bus Access Layer (BAL) must have this system setting configured correctly. MediaCentral Platform Services v2.8 changes this port used in previous releases from 9500 to 9900. To maintain integration between MediaCentral Platform Services and Interplay MAM v5.6, you must verify the correct port has been entered in the MAM system settings.

This setting should only need to be verified with Interplay MAM v5.6. MAM v5.7 includes the correct port for MediaCentral Platform Services v2.8 and later.

For more information, see the "Changing the Setting for the ACS Gateway Port" section of the *Interplay | MAM Installation Manual*.

Reconfiguring MCS for Upgrades from ICS v1.7 or Earlier

In previous releases, the MCPS Player embedded in MediaCentral | UX required its own user name and password for communicating with the MCS server (from which it receives video). This functionality changed in ICS v1.8, where the MCPS Player uses the credentials of the logged-in user.

As a result, if you have deployed MCS in support of Interplay | MAM or Media Composer | Cloud, and are upgrading from ICS v1.7 (or earlier) you will need to reconfigure the MCS System Settings to support these applications.

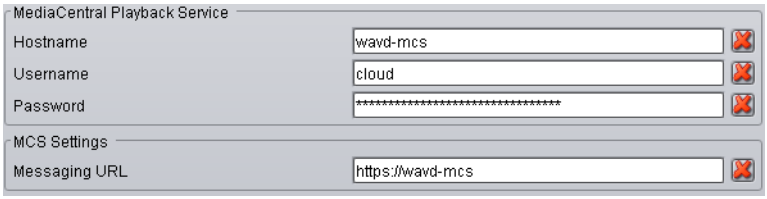
Reconfiguring MCS for Use with Media Composer | Cloud

1. With the MCS server up and running, sign in to MediaCentral UX as a user with administrator-level access.
2. Select System Settings from the Layout selector.
3. In the Settings pane, select MCPS > Player.
4. Media Composer | Cloud User: Enter the user name and password for the Cloud user.

   Suggested User name: cloud

   As a reminder, the Cloud user is a custom account which is added here and in the Interplay (Production) Administrator.

   Example screen shot of the related section of the v3.5 Interplay Administrator:



   This must be a unique user created solely for this purpose. This user should not be created as an Interplay Production or an Avid shared storage system (Avid ISIS or Avid NEXIS).

If the credentials do not match, the Media Composer | Cloud console will present a "Sphere XKAsset Error: 6" indicating an invalid username and password.

Reconfiguring MCS for Use with Interplay | MAM

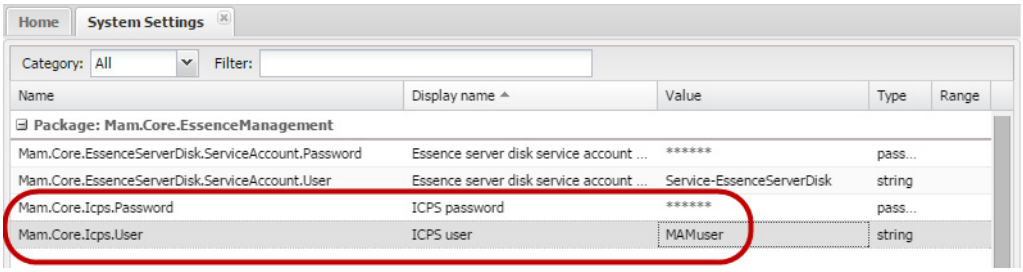
1. With the MCS server up and running, sign in to MediaCentral UX as a user with administrator-level access.
2. Select Users from the Layout selector.
3. Create a special role for the MAM user by clicking on the Create Role button in the Roles pane.
4. Click the Create Role button.
5. In the Details pane, type the properties for the new role:
   - Role name (e.g. MAM)
   - Advance License
   - Do not assign the MAM role any layouts
6. Click Apply to save your changes.

   The new MAM role is added to the Roles pane.
7. Create the MAM system user by clicking the Create User button.
8. In the Details pane, type the properties for the new user:
   - User name (e.g. MAMuser)
   - Password
   - Uncheck "User must change password at next sign-in"
   - Check "User cannot change password
9. Drag the MAM role from Roles pane to the Role section of the Details pane for the new user.

10. Click Save to save your changes.

    The new MAM user is added to the User Tree, as a top-level user.

11. Ensure the System Settings on the Interplay | MAM system are configured to make use of the assigned user name and password. Example:



    See the *Avid MediaCentral | UX Administration Guide* for more information about user creation and role assignment.

Resetting Layouts After Upgrading from v2.0 to v2.10

Three panes used in MediaCentral UX v2.0 were dropped as of MediaCentral UX v2.1:

- Markers pane: redesigned as Logging pane.
- Layouts pane in Users Layout: replaced by drag-and-drop functionality.
- Search pane in Users Layout: replaced by Filter field.

After Media Central UX is upgraded to v2.10, users who had signed out of v2.0 with these panes open will see them when they sign in again, with the message: “No View implementation found for type undefined” in the pane. Users need to reset the panes.

To reset the outdated panes, do one of the following:

- Close the outdated panes.
- Reset the layout by selecting Reset Layout from the Layout selector.

Resetting Layouts After Upgrading from ICS v1.6 or Earlier

After upgrading from Interplay Central Services v1.6 or earlier, users who had previously signed in will see the Assets pane and Search panes from their most recent session. However, the Assets tabs and Search panes are not usable.

This problem does not occur when upgrading from ICS v1.7 or later.

To reset the Assets pane and Search panes, do one of the following:

- Close all open Assets tabs and Search panes and reopen them.
- Reset the layout by selecting Reset Layout from the Layout selector.

Clearing the Browser Cache

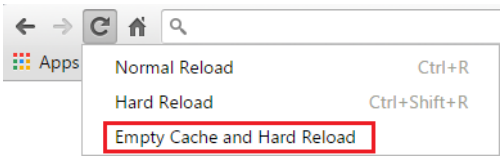
If the user experiences strange behavior or panes with stale data after upgrading MediaCentral, Avid recommends clearing the browser cache as an initial troubleshooting step. Once the client's local cache is cleared, the browser is forced to obtain a new copy of the data from the upgraded MCS server.

While this process is not required for the majority of MCS upgrades and is not required for any specific upgrade path, clearing the cache ("hard-reload") might be beneficial for some edge cases.

Clearing the Cache in Chrome

To hard-reload the local Chrome browser:

1. Open the Chrome browser.
2. Press the F12 key on the keyboard to open the Chrome Console.
3. Right-click on the Reload button in the tool bar and select "Empty Cache and Hard Reload".



4. Close and relaunch the browser to access MediaCentral UX.

Clearing the Cache in Safari

To hard-reload the local Safari browser:

1. Open the Safari browser.
2. Open Preferences from the application's menu and select Privacy.
3. Click the Details button that appears under "Remove All Website Data…".
4. In the popup, type in the name of the upgraded MCS server in the search filter.
5. Once the server is located in the search, select it and click the Remove button in the bottom-left.
6. Press "Option+Cmd+E to empty the browser cache.
7. Close and relaunch the browser to access MediaCentral UX.

B Mounting and Unmounting a USB Drive

Refer to the following instructions to mount and unmount a USB drive from the MCS server.

To mount a USB drive:

1. Connect the drive to an available USB port on the MCS server.
2. Through a Linux command prompt, verify the name of the device using the `dmesg` command:

   `dmesg`

   Information related to the USB drive will appear near the end of the output (close to the list of SCSI devices). The name of the USB drive is found inside square brackets (e.g. `[sdc]`). This is the name you use to mount the drive.
3. If needed, create a mount point for the USB drive:

   `mkdir <path>`

   Where *`<path>`* is the directory to which you want to mount the USB device. Throughout this process, `/media/usb` is used as an example:

   `mkdir /media/usb`
4. Mount the USB drive to the desired mount point:

   `mount /dev/sdc1 /media/usb`

   Note that the name of the USB drive, sdc (in this case), takes a 1 (one) in the mount command. This indicates that a partition exists on the USB drive. When the USB drive was formatted, the partition was created.

   The USB drive is now mounted and available for use.
5. Verify that the USB drive has been mounted:

   `df -h`

   Information is displayed about all mounted file systems and devices, including information about the USB drive, similar to the following (some output omitted, for clarity):

   ```
   Filesystem            Size  Used Avail Use% Mounted on
   /dev/sdc1             7.5G  5.3G  2.2G  71% /media/usb
   ```
6. Use the `cd` command to change to the mount point:

   `cd /media/usb`
7. If desired, copy any files or folder to or from the USB drive.

   For details, see "Copying Software Using a USB Drive" on page 54.

To unmount a USB drive:

1. The USB drive cannot be unmounted from the system if it is the active directory. To avoid issues removing the device, change to the home directory:

   `cd`

In Linux the `cd` *command without any arguments takes you directly to the user's home directory. If you are logged in as root, it takes you to the* `/root` *directory. You must be off the USB drive to unmount it.*

2. Unmount the USB drive:

   `umount /media/usb`

   The USB drive is now available for use in another server.

   If you receive an error message indicating that the USB device is busy, it typically means that the Linux ISO on the USB drive was auto-mounted. Verify what is mounted using the `df -h` command and/or the `mount` command. The Linux ISO is generally mounted to the `/sysinstall` directory.

   Use the following two commands to dismount the Linux ISO, followed by the USB device:

   `umount /sysinstall`

   `umount /media/usb`

3. Disconnect the USB drive from the server.

   Removing the USB drive prevents accidental rebooting and re-imaging of the system disk.

The MCS Installation USB Drive contains a bootable Linux ISO image. If you re-boot the server with the USB drive still in place, RHEL will be re-installed and all your work will be lost. Once you have copied the necessary software, make sure to unmount and remove the USB drive from the server.

C Copying Software to the MCS Server

At various times during the upgrade, you will need to copy software to the MCS server. The following two processes are provided as examples of how to complete this task:

- Using a Windows system and a SFTP tool such as WinSCP
- Connecting a USB drive directly to the server

Copying Software Using WinSCP

To copy software using WinSCP:

1. Download and install the WinSCP software on a Windows system that has network access to the MCS server.

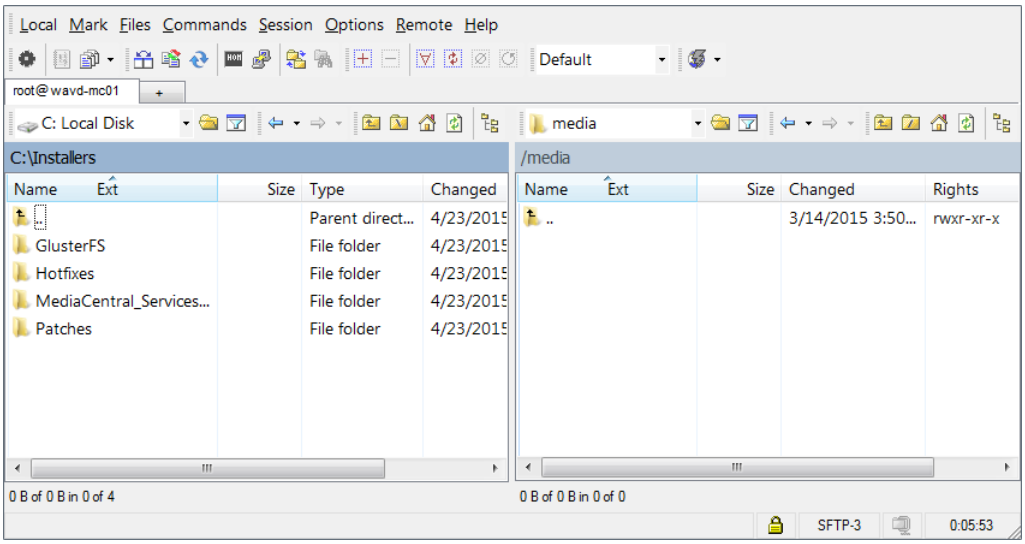
   The WinSCP software can be found at: http://winscp.net.

2. Launch WinSCP.
3. Click the New button and enter the Host name (or IP address) of your server, User name (root), and Password.
4. Click Login.

   The following warning message is displayed: “Continue connecting and add host key to the cache?”

5. Click Yes.

   The WinSCP interface is displayed. The left pane represents your source Windows system. The right pane represents your MCS server.



6. Navigate to the location of the downloaded MCS installation files in the left pane.

7. Navigate to the `/media` folder on the MCS server in the right pane.
8. Create a directory structure for the MCS installer on the MCS server:
   a. Right-click in the right pane and select New > Directory.
   b. In the "New folder name" field, type **`installers`** and click OK.
   c. Double-click on the new `installers` folder in the right pane.
   d. When copying the MCS installer to the server, the software must be contained in its own folder. Create a sub folder for the MCS installer.

      Example: `/media/installers/MCS_2.10`

When manually creating folders, avoid spaces and other illegal Linux characters. Installations will fail if spaces or illegal characters are encountered in the file path.

   e. Drag and drop the files or folders you wish to copy from the left pane to the right.

      Depending on your WinSCP settings, you might see a dialog box asking if you want to copy the files to the remote directory. If asked, click Copy.
9. After all desired files or folders have been copied, close WinSCP.

Copying Software Using a USB Drive

To copy software using a USB drive:

1. Mount the USB drive to the Linux server.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.
2. Create a directory structure for the MCS installer on the MCS server:

   `mkdir /media/installers`
3. When copying the MCS installer to the MCS server, the software must be contained in its own folder. Create a sub folder for the MCS installer:

   `mkdir /media/installers/MCS_2.10`

When manually creating folders, avoid spaces and other illegal Linux characters. Installations will fail if spaces or illegal characters are encountered in the file path.

4. Copy files to the MCS server:

   For a single file: **`cp <filename> /media/installers/MCS_2.10`**

   For a folder: **`cp -R <foldername> /media/installers/MCS_2.10`**
5. Once you have finished copying all necessary files, unmount the USB drive.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

D Deleting the RAID 5 Array

When upgrading from one version of RHEL to another, such as an upgrade from RHEL v6.3 to RHEL v6.5, you must delete the RAID 5 prior to installing the new operating system and MCS software. Deleting and re-creating the RAID 5 eliminates (in advance) any problems with cache permissions that can arise as a result of the RHEL update.

This section provides instructions for deleting the RAID 5. For information on re-creating the RAID 5, see "Configuring the Onboard RAID" in the *MediaCentral Platform Services Installation and Configuration Guide*.

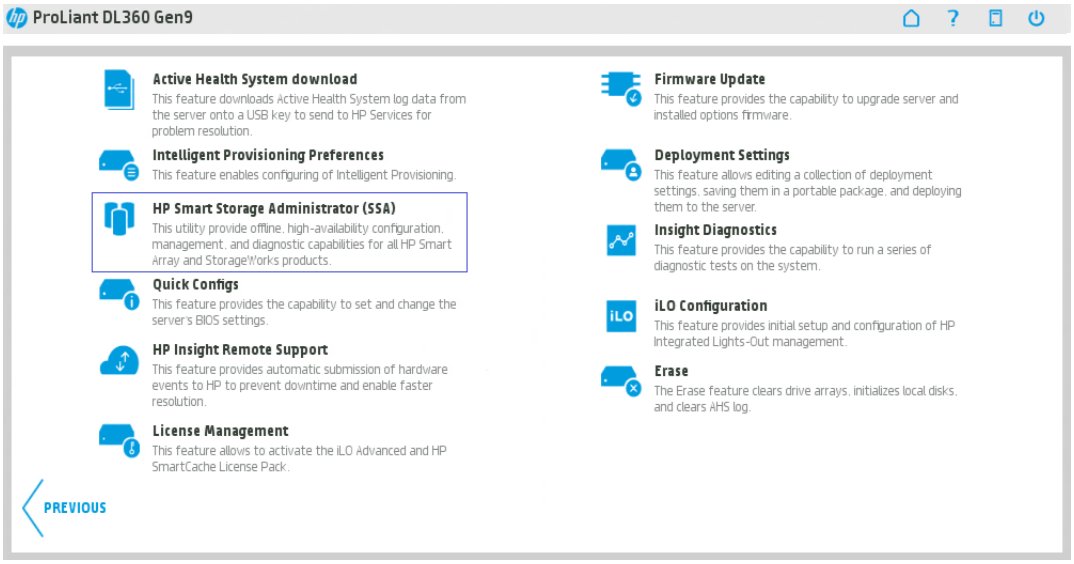
Refer to one of the following sections as it applies to your server platform:

- "Deleting the RAID 5 on an HP Gen9" on page 55
- "Deleting the RAID 5 on an HP Gen8" on page 56
- "Deleting the RAID 5 on a Dell Server" on page 59

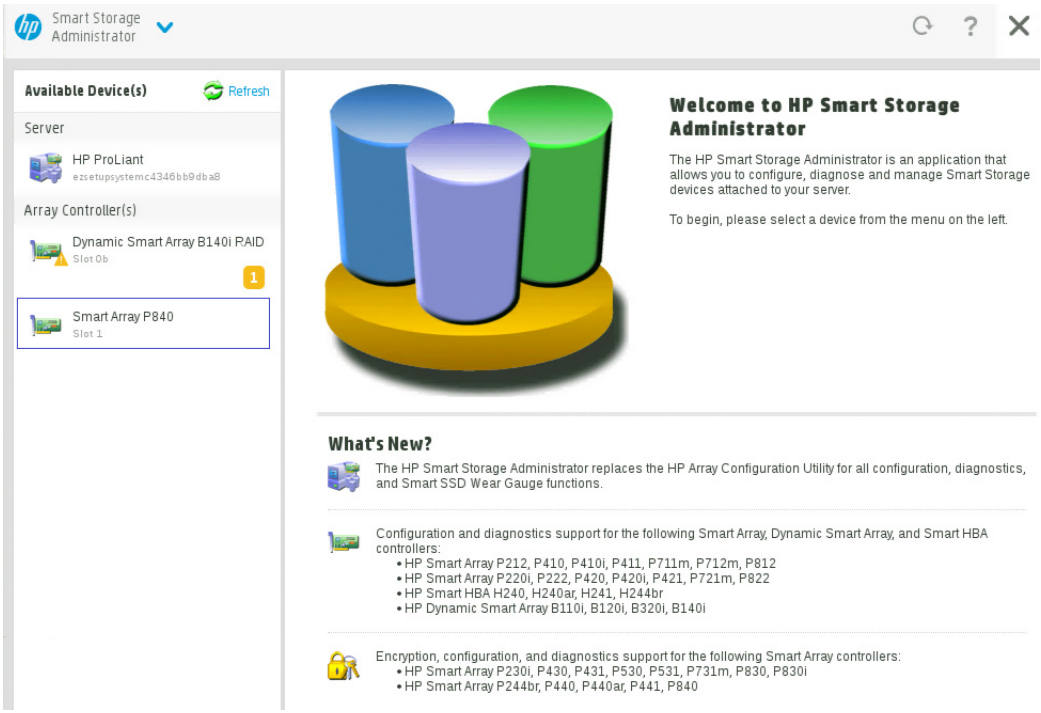
Deleting the RAID 5 on an HP Gen9

To delete the RAID 5 on an HP Gen9 server:

1. Reboot the server and press F10 to select **Intelligent Provisioning**.
2. Select the **Perform Maintenance** option.
3. Select **HP Smart Storage Administrator (SSA)**.


ProLiant DL360 Gen9
Active Health System download
This feature downloads Active Health System log data from the server onto a USB key to send to HP Services for problem resolution.
Intelligent Provisioning Preferences
This feature enables configuring of Intelligent Provisioning.
HP Smart Storage Administrator (SSA)
This utility provide offline, high-availability configuration, management, and diagnostic capabilities for all HP Smart Array and StorageWorks products.
Quick Configs
This feature provides the capability to set and change the server's BIOS settings.
HP Insight Remote Support
This feature provides automatic submission of hardware events to HP to prevent downtime and enable faster resolution.
License Management
This feature allows to activate the iLO Advanced and HP SmartCache License Pack.
Firmware Update
This feature provides the capability to upgrade server and installed options firmware.
Deployment Settings
This feature allows editing a collection of deployment settings, saving them in a portable package, and deploying them to the server.
Insight Diagnostics
This feature provides the capability to run a series of diagnostic tests on the system.
iLO Configuration
This feature provides initial setup and configuration of HP Integrated Lights-Out management.
Erase
The Erase feature clears drive arrays, initializes local disks, and clears AHS log.
PREVIOUS

4. At the “Welcome to HP Smart Storage Administrator” screen, select **Smart Array P840** from the Available Devices menu on the left.

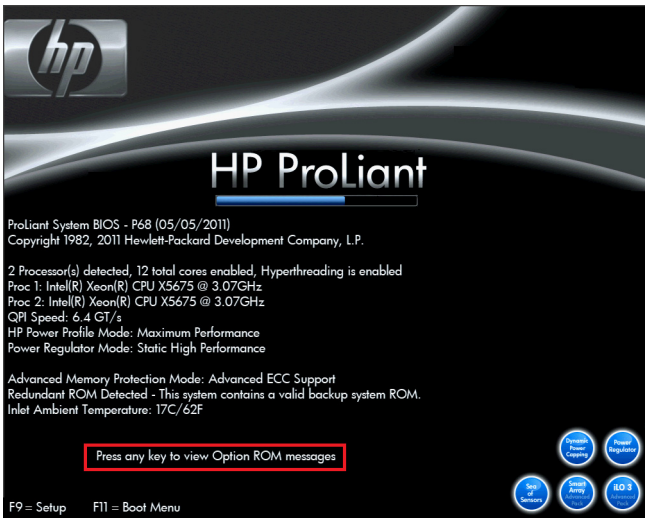

Smart Storage Administrator
Available Device(s)
Refresh
Server
HP ProLiant
Array Controller(s)
Dynamic Smart Array B140i RAID
Slot 0b
Smart Array P840
Slot 1
Welcome to HP Smart Storage Administrator
The HP Smart Storage Administrator is an application that allows you to configure, diagnose and manage Smart Storage devices attached to your server.
To begin, please select a device from the menu on the left.
What's New?
The HP Smart Storage Administrator replaces the HP Array Configuration Utility for all configuration, diagnostics, and Smart SSD Wear Gauge functions.
Configuration and diagnostics support for the following Smart Array, Dynamic Smart Array, and Smart HBA controllers:
• HP Smart Array P212, P410, P410i, P411, P711m, P712m, P812
• HP Smart Array P220i, P222, P420, P420i, P421, P721m, P822
• HP Smart HBA H240, H240ar, H241, H244br
• HP Dynamic Smart Array B110i, B120i, B320i, B140i
Encryption, configuration, and diagnostics support for the following Smart Array controllers:
• HP Smart Array P230i, P430, P431, P530, P531, P731m, P830, P830i
• HP Smart Array P244br, P440, P440ar, P441, P840

5. Use the Smart Array utility to delete the existing RAID5.

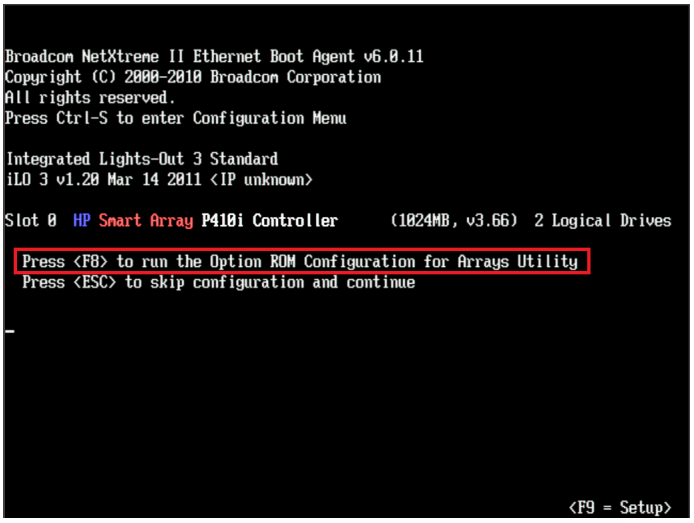
Deleting the RAID 5 on an HP Gen8

To delete the RAID 5 on an HP Gen8 server:

1. Reboot the MCS server.
2. Press any key when prompted (space-bar recommended) to display the HP ProLiant “Option ROM” messages.

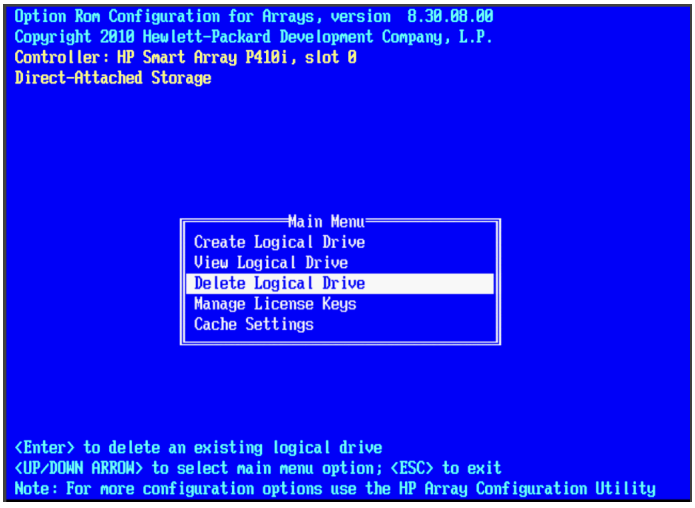

HP ProLiant
ProLiant System BIOS - P68 (05/05/2011)
Copyright 1982, 2011 Hewlett-Packard Development Company, L.P.
2 Processor(s) detected, 12 total cores enabled, Hyperthreading is enabled
Proc 1: Intel(R) Xeon(R) CPU X5675 @ 3.07GHz
Proc 2: Intel(R) Xeon(R) CPU X5675 @ 3.07GHz
QPI Speed: 6.4 GT/s
HP Power Profile Mode: Maximum Performance
Power Regulator Mode: Static High Performance
Advanced Memory Protection Mode: Advanced ECC Support
Redundant ROM Detected - This system contains a valid backup system ROM.
Inlet Ambient Temperature: 17C/62F
Press any key to view Option ROM messages
F9 = Setup
F11 = Boot Menu

3. As soon as you see the prompt to enter the Option ROM Configuration for Arrays utility, press F8.

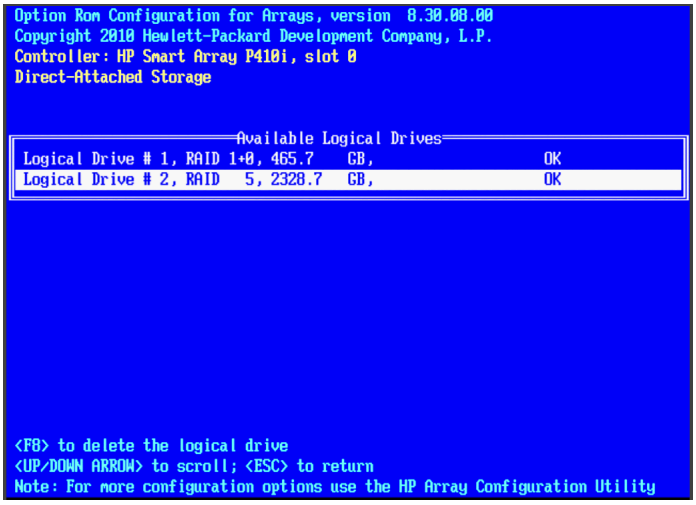

Broadcom NetXtreme II Ethernet Boot Agent v6.0.11
Copyright (C) 2000-2010 Broadcom Corporation
All rights reserved.
Press Ctrl-S to enter Configuration Menu
Integrated Lights-Out 3 Standard
iLO 3 v1.20 Mar 14 2011 <IP unknown>
Slot 0 HP Smart Array P410i Controller (1024MB, v3.66) 2 Logical Drives
Press <F8> to run the Option ROM Configuration for Arrays Utility
Press <ESC> to skip configuration and continue
<F9 = Setup>

The prompt to press F8 can flash by very quickly. If you miss it, reboot and try again.

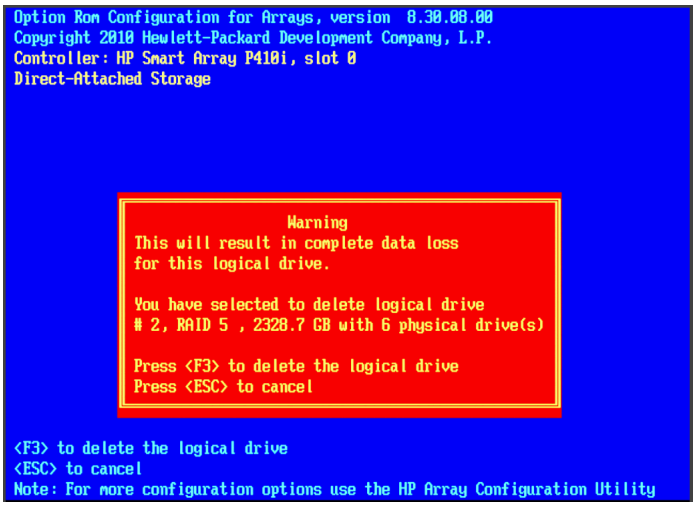
4. From the Main Menu, select Delete Logical Drive and press Enter.


Option Rom Configuration for Arrays, version 8.30.00.00
Copyright 2010 Hewlett-Packard Development Company, L.P.
Controller: HP Smart Array P410i, slot 0
Direct-Attached Storage
Main Menu
Create Logical Drive
View Logical Drive
Delete Logical Drive
Manage License Keys
Cache Settings
<Enter> to delete an existing logical drive
<UP/DOWN ARROW> to select main menu option; <ESC> to exit
Note: For more configuration options use the HP Array Configuration Utility

5. Select the RAID 5 and press F8 to delete.


Option Rom Configuration for Arrays, version 8.30.08.00
Copyright 2010 Hewlett-Packard Development Company, L.P.
Controller: HP Smart Array P410i, slot 0
Direct-Attached Storage
Available Logical Drives
Logical Drive # 1, RAID 1+0, 465.7 GB, OK
Logical Drive # 2, RAID 5, 2328.7 GB, OK
<F8> to delete the logical drive
<UP/DOWN ARROW> to scroll; <ESC> to return
Note: For more configuration options use the HP Array Configuration Utility

6. A warning appears asking you to confirm your choice. Press F3 to delete the RAID.


Option Rom Configuration for Arrays, version 8.30.08.00
Copyright 2010 Hewlett-Packard Development Company, L.P.
Controller: HP Smart Array P410i, slot 0
Direct-Attached Storage
Warning
This will result in complete data loss
for this logical drive.
You have selected to delete logical drive
2, RAID 5 , 2328.7 GB with 6 physical drive(s)
Press <F3> to delete the logical drive
Press <ESC> to cancel
<F3> to delete the logical drive
<ESC> to cancel
Note: For more configuration options use the HP Array Configuration Utility

7. The RAID 5 is removed, and can now be re-created.

   For more information, see “Configuring the Onboard RAID” in the *MediaCentral Platform Services Installation and Configuration Guide*.

As indicated in the MediaCentral Platform Services Installation and Configuration Guide, once you have re-created the RAID 5 and have returned to the Main Menu, do not press <Esc> to exit since this reboots the server. Wait until you have inserted the USB drive and are ready to perform the upgrade.

Deleting the RAID 5 on a Dell Server

Deleting and recreating the RAID sets using the DELL BIOS utility does not erase data, nor does it delete existing partitions. That is, deleting a RAID does not delete the partition table — unless you initialize the disk at the same time. However, initializing the disk is a slow process.

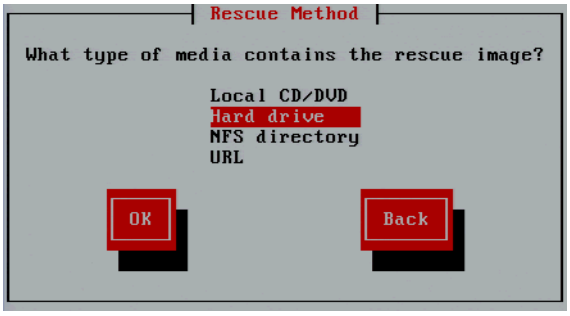
In this procedure, you boot from the MCS Installation USB Drive and launch a RHEL “rescue” session to identify and delete the current system partitions.

To delete the RAID 5 on a Dell server:

1. Connect the MCS Installation USB drive to the MCS system the boot the server.
2. At the RHEL Welcome screen, select “Rescue Installed System”.

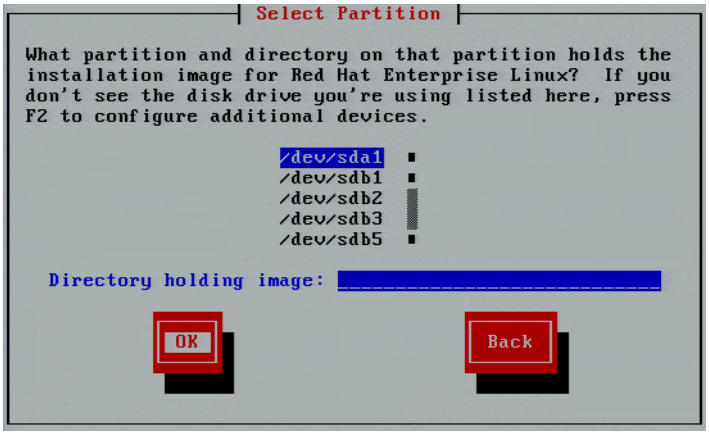
Welcome to Red Hat Enterprise Linux 6.5!
Install Red Hat 6.5 with ICS
Upgrade to Red Hat 6.5
Rescue installed system
Boot from local drive
Memory test
Press [Tab] to edit options
RED HAT
ENTERPRISE LINUX 6
Copyright © 2003-2010 Red Hat, Inc. and others. All rights reserved.

3. When prompted choose the language and keyboard.
4. Choose “Hard drive” as the rescue method and select OK.

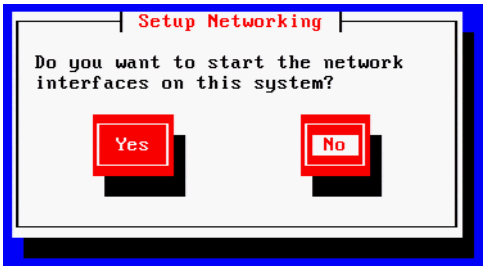


For the purposes of booting from a RHEL image, the USB drive is considered a hard drive.

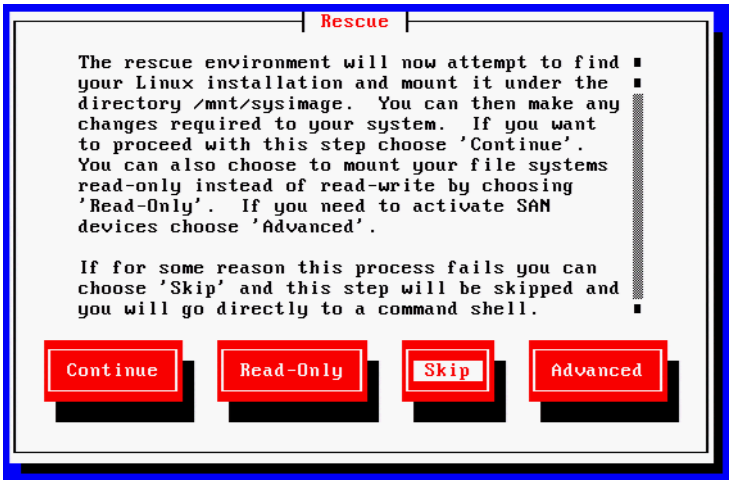
5. Select the "/dev/sda1" partition (the USB drive) and select OK. Leave the "Directory holding image" field blank.


Select Partition
What partition and directory on that partition holds the installation image for Red Hat Enterprise Linux? If you don't see the disk drive you're using listed here, press F2 to configure additional devices.
/dev/sda1
/dev/sdb1
/dev/sdb2
/dev/sdb3
/dev/sdb5
Directory holding image:
OK
Back

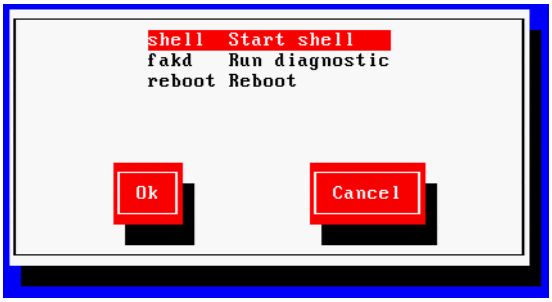
6. Select No in the Setup Networking window and press Enter on the keyboard. Networking support is not required at this time.



7. Select "Skip" in the Rescue window and press Enter on the keyboard.


Rescue
The rescue environment will now attempt to find your Linux installation and mount it under the directory /mnt/sysimage. You can then make any changes required to your system. If you want to proceed with this step choose 'Continue'. You can also choose to mount your file systems read-only instead of read-write by choosing 'Read-Only'. If you need to activate SAN devices choose 'Advanced'.
If for some reason this process fails you can choose 'Skip' and this step will be skipped and you will go directly to a command shell.
Continue
Read-Only
Skip
Advanced

8. At the next screen, choose “shell Start shell” and select OK.



9. At the system prompt, use the RHEL fdisk utility to examine the current partitions:

   `fdisk -cul`

   This command will display the available disks and partitions on the system. Since scroll bars will not be present in the rescue shell, use Shift-Pg Up and Shift-Pg Down to view the entire output.

   In this case “sda” should be the USB boot drive, “sdb” should be the RAID 1 volume and “sdc” should be the RAID 5 volume.

   The following example shows information for “sdb” with three partitions (sdb1, sdb2, sdb3):

```
Disk /dev/sdb: 500.1 GB, 500074307584 bytes
255 heads, 63 sectors/track, 60797 cylinders, total 97670732 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xc755f5b0

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1   *        2048     1026047      512000   83  Linux
/dev/sdb2         1026048    42051583    20512768   8e  Linux LVM
/dev/sdb3        42051584   976707583   467328000   8e  Linux LVM
```

   Additional entries for the file system (sdb4, sdb5) could also be possible. Example:

```
Disk /dev/sdb: 598.9 GB, 598879502336 bytes
255 heads, 63 sectors/track, 72809 cylinders, total 11696828 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x930a8a0e

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1   *        2048     1026047      512000   83  Linux
/dev/sdb2         1026048     2050047      512000   83  Linux
/dev/sdb3         2050048    43075583    20512768   8e  Linux LVM
/dev/sdb4        43075584  1169686527   563305472    5  Extended
/dev/sdb5        43077632  1169686527   563304448   8e  Linux LVM
```

Delete any partitions on the RAID 1 volume and the RAID 5 volume (if applicable). The remaining steps in this process will assume “sdb” is the RAID 1 and “sdc” is the RAID 5.

10. Use the RHEL `fdisk` utility to select the sdb volume:

    `fdisk /dev/sdb`

11. Type: **`p`** to print the current file system partition table. This will show you a similar output as the `fdisk -cul` command you used earlier.
12. Type: **`d`** to begin deleting the partitions.
13. You will be prompted to specify the partition to delete. Example: **`1`**

    `Partition number (1-4):` **`1`**

14. Repeat the above two steps to delete all remaining “sdb” partitions.
15. Once complete, type **`p`** to print the partition table again. An empty partition table should look like the following:

    Device Boot Start End Blocks Id System

16. Type: **`w`** to write the changes to the partition table and exit the utility.
17. If you have a RAID 5 volume, repeat this process by specifying the RAID 5 “sdc” partition:

    `fdisk /dev/sdc`

18. Repeat the above steps and type **`w`** to write the changes to the partition table and exit the utility.
19. Verify that the partitions on sdb and sdc (if applicable) were successfully removed using the RHEL fdisk utility:

    `fdisk -cul`

E Working with Media Index

This section covers additional topics related to upgrades that include Media Index.

Verifying the Media Index Status

Before you upgrade a MediaCentral system configured with Media Index, you need to ensure that there is no active schema migration currently affecting Media Index. When you change a field set of the system (Interplay Production, iNEWS, or Interplay Archive) and the change propagates to Media Index, any existing data is automatically migrated to reflect the changes. For large indexes, schema migration can take a while. To avoid an inconsistent Media Index state, you need to make sure that there is no schema migration actively affecting your indexes.

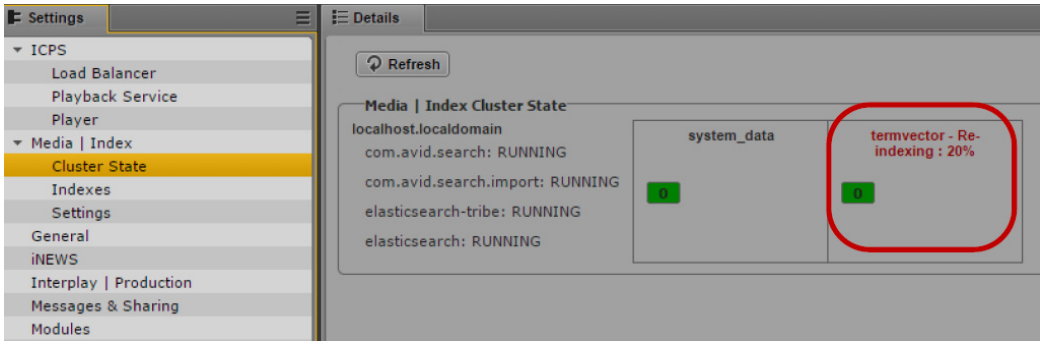
Once any current migration completes, you can continue with the MCS upgrade procedures.

To check the migration status prior to upgrading:

1. Sign in to MediaCentral UX as an administrator.
2. Select System Settings from the Layout selector.

   The System Settings layout opens.
3. In the Settings pane select Media Index > Cluster State.

   The Media Index Cluster State displays in the Details pane.
4. Check the cluster state:
   a. If there is no active migration, all index labels appear in black.
   b. If the index has an active migration, its label appears in red with an indication of the migration progress.



5. If there is active migration is in progress, wait for the process to finish before proceeding with the MCS upgrade procedures.

Stopping and Starting the PEBCo Agent

Some upgrade paths require the user to stop the indexing of the Interplay Production or Interplay Archive database prior to upgrading MediaCentral Platform Services. Once the upgrade is complete, the process must be manually restarted. Complete the single-server or cluster process below if it applies to your upgrade.

Stopping the PEBCo Agent

Prior to updating the MediaCentral server, stop the PEBCo agent in the Interplay Administrator to pause the indexing of the Interplay Production database. Complete this step for each indexed Interplay Production and / or Interplay Archive system.

To stop the PEBCo agent:

1. Log into the Interplay Administrator on the Interplay Production Engine.
2. Click the Production Engine Bus Connector icon under the Site Settings section.

The Production Engine Bus Connector view is not available on Macintosh clients.

3. Under the Manage/Status tab, click the Stop button to stop the PEBCo agent.

To verify the names of the configured Interplay Production systems, review the Media Index "Indexes" in the MediaCentral UX System Settings.

4. Complete the upgrade to the MCS server as outlined in the body of this guide.

Starting the PEBCo Agent

Once the upgrade to the MediaCentral servers is complete, you must re-enable indexing of the Interplay database by starting the PEBCo Agent. This step must be completed for each indexed Interplay Production and Interplay Archive database.

Interplay Administrator v3.5 or later must be used to complete this process. You do not need to update your Interplay Production Engine to v3.5, but you must have the Interplay Administrator tool that installs with Interplay Access v3.5 or later to enable sync events for Media Index. If you are indexing an Interplay Archive database, Interplay Administrator v3.6 or later is required.

To restart the PEBCo agent:

1. Log into the Interplay Administrator on the Interplay Production Engine.
2. Click the Production Engine Bus Connector icon under the Site Settings section.
3. Under the Manage/Status tab, click the Start button to restart the PEBCo agent.

F Verifying System Configuration Files

MediaCentral Platform Services includes multiple configuration files which govern the behavior of the system services. Some of these files can be modified to include custom modifications.

During a system upgrade, the MCS installer checks the configuration files to determine if any custom modifications have been made. If no modifications are found, the files are overwritten. If the installer finds a modified file, the original "filename" is left unaltered and a "filename.rpmnew" is created in the same directory. In some cases, the installer script also alerts the user to the .rpmnew file creation with a message similar to the following:

```
warning: /usr/maxt/maxedit/etc/edit.cfg created as /usr/maxt/maxedit/etc/
edit.cfg.rpmnew
```

When a .rpmnew file is created, you must manually migrate the custom modifications from the original file to the newly created .rpmnew file. If the modifications are not migrated to the new file, system functionality and stability might be affected.

To review and update configuration files:

1. Open an SSH connection to the MCS single-server or cluster master node using a SSH client such as PuTTY.
2. Log in to Linux as the 'root' user.
3. List the contents of the following directories to determine if any `.rpmnew` files exist:

   `ls /usr/maxt/maxedit/etc`

   `ls /etc/sysconfig/`

   If any configuration files have been modified, both a `<filename>` and a `<filename>.rpmnew` file will exist in the same directory.

Alternatively, you can limit the output of the list command to display only rpmnew files using the following command: `ls /<path> |grep rpmnew`

   If you do not see any `.rpmnew` files, no custom modifications were made and this process does not apply to your MediaCentral environment.

   If a `<filename>.rpmnew` file is present, continue to step 4.

4. You will need to compare the contents of the two files and migrate any custom modifications from `<filename>` to `<filename>.rpmnew`. To accomplish this task, open a second SSH connection to the MCS server in a different window.
5. In the first SSH window, list the contents of the `<filename>` file:

   `cat /<path>/<filename>`

6. In the second SSH window, open `<filename>.rpmnew` for editing:

   `vi /<path>/<filename>.rpmnew`

7. Compare the contents of the files and migrate any custom modifications to the `.rpmnew` file.

Different versions of the same file might include additional variations beyond the custom modifications. Only migrate the custom data to the new file. If you are unsure what data should be migrated to the new file, contact Avid Customer Care.

8. Once the edits are complete, save and exit the vi session. Press <ESC> and type: **`:wq`**
9. Rename the existing *`<filename>`* to *`<filename>`*`.old`:

   `mv <filename> <filename>.old`

Alternatively, the older copy of the file could be deleted at this time as it is no longer necessary.

10. Rename the *`<filename>`*`.rpmnew` file to *`<filename>`*:

    `mv <filename>.rpmnew <filename>`

11. If you are running a clustered configuration, repeat steps 1 – 10 on all cluster nodes.

Alternatively to save time and avoid errors during the text editing process, the modified file or files can often be copied to the other nodes.

12. Once complete, the avid-all service must be restarted:
    - For a single MCS server, restart the service through the avid-ics script:

      `avid-ics restart`

    - For a clustered configuration, return to "Updating the Cluster" on page 26 to continue the upgrade. The avid-all service is restarted later in the process when bringing the cluster back online.

G Backing Up and Restoring System Settings and the ICS/MCS Database

Before performing an upgrade it is recommended — and sometimes required — that you back up the ICS/MCS system settings and database using the `system-backup` script. Depending on the upgrade path, you may also be required to restore the data once the upgrade is complete.

The `system-backup` script backs up important files and directories, including network settings, cluster configuration files, and more. In addition, the script calls the `avid-db` command, which dumps and backs up the contents of the ICS/MCS database. The ICS/MCS database contains data related to ACS (Avid Common Services, "the bus"), UMS (User Management Service) and ICPS (Interplay Central Playback Services) data.

In a cluster, the ICS/MCS database is replicated between the master and slave nodes, but it is only ever mounted on the master node. Thus, the ICS/MCS database is only available for dumping and backup on the master node.

If you are backing up multiple nodes in a cluster, rename the backup file for each node before proceeding to the next node. If you do not rename the backup file, it will be overwritten by the backup on the next node. This is particularly problematic if the master node's backup file is overwritten, as this is the only backup that contains a copy of the MCS database.

The following table lists the files and directories backed up and restored by the system-backup script. The table lists files as they are found in the `ics_setup_files.tar.gz` backup file:

Directory/File	Description
/etc/bucardorc	Bucardo configuration file used for database replication in a cluster
/etc/collectd.conf	Configuration file for the collectd service
/etc/localtime	Time zone info
/etc/ntp.conf	/etc/ntp.confNetwork Time Protocol config file
/etc/redis.conf	Configuration file for the redis service
/etc/resolv.conf	DNS config file
/etc/sudoers	List of users with sudo privileges
/etc/collectd.d/	Configuration files for the collectd service
/etc/corosync/corosync.conf	Corosync config file (cluster only)
/etc/cron.d/ntpd	The cron job that automates synchronization of the system clock.
/etc/drbd.d/r0.res	DRDB config file (cluster only)
/etc/elasticsearch/ /etc/elasticsearch-tribe/	Settings related to Media Index

Directory/File	Description
/etc/pgpool-II/	Settings related to Multi-Zone configs
/etc/rsyslog.d/	Configuration file pertaining to the ICPS service
/etc/security/	
/etc/snmp/	Simple Network Management Protocol (network monitor)
/etc/sudoers.d/	List of users with sudo privileges
/etc/sysconfig/	Network settings and more
/etc/udev/rules.d/70-persistent-net.rules	NIC card settings
/opt/avid/etc/avid/avid-interplay-central/ssl/jetty.keystore	SSL private key file used with MCS 2.4 and earlier.
/opt/avid/etc/pki/certs/site.crt /opt/avid/etc/pki/private/site.key	SSL Certificate (site.crt) and private key (site.key) files used with MCS 2.5 and later.
/opt/avid/etc/avid/avid-interplay-central/config/application.properties	Contains customized options for MCS.
/root/	Filesystem settings originally obtained from /etc/fstab
/usr/maxt/maxedit/etc/*	Maxedit settings (used by ICPS)
/usr/maxt/maxedit/share/MPEGPresets/MPEG2TS.mpegpreset	Defines encoding for iOS playback
/var/lib/avid/db/dumps /var/lib/avid/db/mongodump/*	ICS/MCS database (ACS, UMS and ICPS data). This includes user information.
RHEL user names and passwords	***** Not backed up. *****

RHEL user names and passwords (such as the root user) are not backed up or restored by the system-backup script. After the upgrade, log in as "root" with the default password of "Avid123".

Completing a Backup

When backing up the master node in a cluster, it must not be in standby mode. If desired, all other slave and load balancing nodes can be in standby.

To back up the system settings and ICS/MCS database:

1. Mount the USB drive containing the system-backup script.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.
2. From a Linux command prompt, navigate to the mount point. For example:

   ```
   cd /media/usb
   ```
3. Back up the ICS/MCS settings and database using the backup script:

   ```
   ./system-backup.sh -b
   ```

   In this case the script is used with the "-b" option which indicates you want to backup the data.

If the following message appears, it indicates that a copy of the `pcmk.conf` *file already exists:*

```
File /root/pcmk.conf exists. Do you want to overwrite it (y/n)?
```

This file contains information about the Corosync cluster. Type "yes" or "y" to overwrite the file or "no" if you do not wish to overwrite the file. In either case, the backup script continues.

A backup file is written to the USB drive:

`/media/usb/sys-backup/ics_setup_files.tar.gz`

Since the system-backup script also calls the avid-db command, a backup of the ICS/MCS database is also written to the following directory (on the ICS/MCS server):

`/var/lib/avid/db/dumps`

The backup file on the server has a name has the following form:

`ALL-YYYYMMDD_HHMMSSZ.sql.gz.cr`

Note the time stamp appended to the file name uses the Universal Time Code (UTC), not the local time.

The following message indicates success:

```
Backup setup successful!
```

4. Make a copy of the backup file using the Linux `cp` command. For example:

   `cp -r sys-backup sys-backup-<nodename>`

   The above command creates a renamed copy of the directory containing the backup file. The backup file itself (ics_setup_files.tar.gz) remains unchanged inside the directory.

Making a copy of the backup file is good practice, and is particularly important if you are backing up multiple nodes in a cluster. Only the master node backup contains a complete set of backup information (including end-user data). If you do not make a copy of the master node backup file, it will be overwritten by the backup from a non-master node.

5. Once the settings are backed up, it is good practice to unmount and remove the USB drive to avoid accidentally rebooting, resulting in a re-image of the system disk.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

6. If you have a cluster configuration, repeat the above steps on all nodes.

Completing a Restore

To restore the system settings and ICS/MCS database:

1. Mount the USB drive containing the system-backup script.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

2. From a Linux command prompt, navigate to the mount point. For example:

   `cd /media/usb`

3. If you made a renamed copy of the backup, restore the original folder name:

   `cp -r sys-backup-<nodename> sys-backup`

4. Restore the ICS/MCS settings and database using the backup script:

   `./system-backup.sh -r`

   In this case the script is used with the "-r" option which indicates you want to restore data.

   You are asked to confirm the restoration of the ICS/MCS database:

   ```
   Would you like to restore the database now? (y/n)
   ```

5. Type "**`y`**" (without the quotes) to confirm the action.

   The script requests confirmation that services can be stopped at this time:

   ```
   All Avid services will be shut down before performing a database restore
   operation.
   Would you like to continue? [yes/no]
   ```

6. Type "**`yes`**" (spelled out in full, without the quotes) to confirm the action.

Be careful when typing your response to this question. Entering anything other than "yes" results in the script exiting without restoring the ICS/MCS database. Other items are restored, but not the ICS/MCS database.

The script is executed. Once complete, the following message is generated:

```
Restoration done!
Your old fstab settings were saved in /root/fstab
Please remove the USB key and reboot the server.
```

The file system table file (fstab) contains information to automate mounting volumes at boot time. It is not restored automatically.

7. Compare the current and restored file system table files "fstab" for changes:

   `cat /<path>/fstab`

   - The current "live" file system table is located at: `/etc/fstab`
   - The restored file system table is located at: `/root/fstab`

   Since some entries in the file are assigned UUIDs dynamically by Linux, the restore script does not place the `fstab` file in its original location. These UUIDs can change from one RHEL installation to the next, even if they underlying hardware remains the same. Therefore it is important to manually compare the contents of the restored file to the original file to ensure all system settings are migrated.

   For example, in an MCS system configured for Interplay | MAM, the fstab file contains an entry to automatically mount the Interplay | MAM file system. This information must be manually added to the active file at: `/etc/fstab`

   Add information to the "live" fstab file as necessary.

The UUID information will be different between "live" and restored fstab files. Do not alter this information.

8. Once the settings are restored, unmount and remove the USB drive.

   For details, see "Mounting and Unmounting a USB Drive" on page 51.

Avid
75 Network Drive
Burlington, MA 01803-2756 USA

Technical Support (USA)
Visit the Online Support Center at www.avid.com/support

Product Information
For company and product information, visit us on the web at www.avid.com